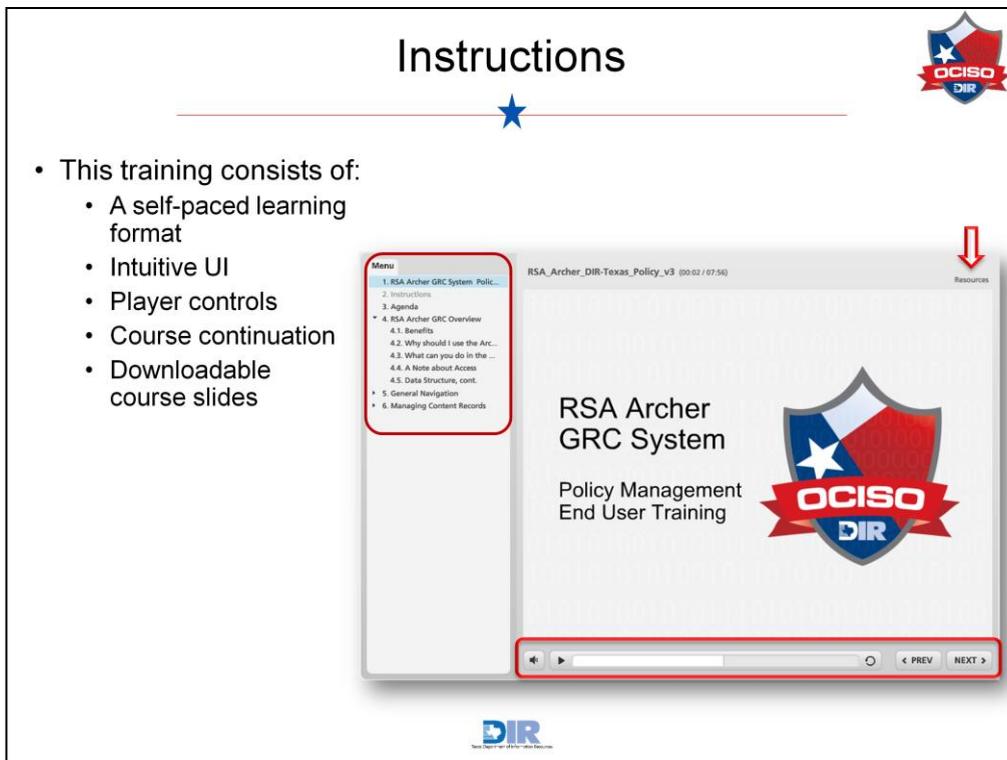


# RSA Archer GRC System

Policy Management  
End User Training



Welcome to the RSA Archer GRC System Policy Management training course.



- This training consists of:
  - A self-paced learning format
  - Intuitive UI
  - Player controls
  - Course continuation
  - Downloadable course slides

This training is presented in a self-paced learning format to offer you convenience and flexibility. If this is your first time taking a course in this format, here are a few tips and instructions:

**User Interface:** the intuitive user interface provides navigational aids to help you make your way through the course. The menu on the left side of the screen lists major sections of the course, as well as all of the slides by title. You may click through in order or jump to any slide or section.

**Player Controls:** the bottom of the screen has player controls for you to start or stop the presentation and to move backwards or forwards through the slides.

**Course Continuation:** you can close the browser window to exit the program completely. If you have not completed the course, you are prompted to resume at the same spot when you return.

**Attachments:** the Resources menu at the top of your screen provides you with a link to downloadable course slides used in this course. The script for the audio portion of this course is included in the notes. You may wish to download the slides to use as a reference at a later time.

# Agenda



- RSA Archer GRC Overview
- General Navigation
- Managing Content Records
- Policy Management
  - Creating a Policy
  - Creating a Control Procedure
  - Creating an Exception Request
- Security Plan Template
  - Creating a Security Plan Template
  - Inline Editing
  - Archived Templates
- Searching & Reporting



This training course will cover the following topics:

- An overview of the RSA Archer GRC system
- General navigation of the interface.
- Instruction on how to manage records in the system.
- Then, we'll get into the use of the RSA Archer GRC system within Texas state organizations for policy management. In this section, we will describe how to create a policy, control procedure, and exception request.
- Next, we'll describe how to create a security plan template, touch on the inline editing feature, and explore archived templates.
- Finally, we'll wrap up with some instruction on how to search for records and save those searches as reports.



# RSA Archer GRC Overview



First, let's talk about the system as a whole.

# Benefits



- Consolidates data into a single location
- Allows data to be updated in one location/propagated in many locations
- Access to data is controlled based on the user logged in
- Email notifications can go out based on data changes
- Record varying levels of information in one location



There are a number of benefits to the RSA Archer GRC system. Archer allows you to consolidate all of your data into a single location that is accessible from anywhere you have internet access, instead of keeping information in spreadsheets, or other local files.

Once you make a change to data in one location, anywhere else that that data is referenced, the information is also updated. This allows you to do things like change the phone number for a person and anywhere that phone number is referenced, it is updated there as well.

Access to data housed in the system can be controlled all the way down to an individual user level. This means that someone at an organization level may only be able to view information related to her organization, but someone in the main DIR office may be able to view information across all organizations.

And finally, the system allows for a lot of business processes to be automated. No longer will you need to manually email someone each time something happens – when you log certain information into the system, the system will automatically send an email for you.

## Why should I use the Archer GRC system?



- All organizations are required to complete a Security Plan biennially
- Gives organizations a place to continually record all security plan information, and provide information to management to comply with TAC 202.23a / TAC 202.73a
- Organizations can keep track of Controls, Findings, and Exception Requests



With Archer, organizations can complete the Security Plan that they are required by legislature to complete biennially. They can also relate Findings to Control Procedures, and create and track Exception Requests and Remediation Plans on a centralized platform.

## What can you do in the Archer GRC system?



- Create Policies and Control Procedures specific to your organization
- Create Exception Requests and Remediation Plans to address Findings
- Assess control maturity levels and plan implementation strategies
- Assist in streamlined reporting efforts across the board



The same processes that have historically been done using email, meetings, and spreadsheets can now be handled through a single system. This ultimately makes roll-up reporting possible and gives the business as a whole better access to policies, authoritative sources, and control maturity levels.

In the system, you will be able to:

- Create Policies and Control Procedures specific to your organization
- Create Exception Requests and Remediation Plans to address Findings
- Assess control maturity levels and plan implementation strategies

There are a large number of reports that have been created for your use. The flexibility of Archer gives you the ability to create and export or print your data in a variety of ways. The information found in this system is confidential. Given the flexibility of the system, we cannot mark everything that is printed from this system as confidential. You will want to mark printed materials from this system according to your organization's classification/confidentiality requirements.

## A Note about Access



- User permissions are role-based
- Users may only do and see what their access allows
- Access can be defined down to an individual field-level
- Just because you can, doesn't mean you should



Some important notes about access within the system:

- User accounts are assigned roles that enable what each user is allowed to do and see. It is entirely possible that two users sitting side by side and logged into their own accounts will see drastically different views of the same or different data.
- User roles simply grant the most possible access allowed to a user. Depending on the status of a record or other factors, user interaction may be further limited.
- Access can be defined all the way down to an individual field level.
- Based on how the system is configured, you may encounter multiple ways to perform similar tasks. For example, a *New* icon may indeed allow you to add a new record, but defined processes may recommend that you create the new records from an alternate location in order for additional relationships between records to be created.

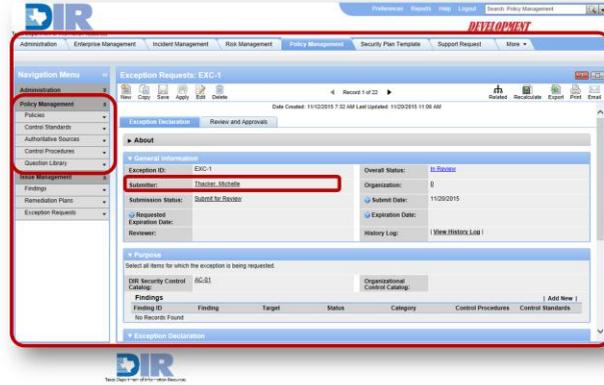
We will talk more about the proper paths to follow as we dig into the DIR-Texas-specific workflows a little later in this course.

# Data Structure, cont.



Within Archer:

- Solution: Overarching tab in the top toolbar
- Application: Subsection within the Solution
- Record: Set of data pertaining to an Application
- Field: Specific piece of information within a Record.



When working with data, it is important to understand Archer terminology as it will be referred throughout this training:

- Policy Management is a **Solution**, often presented as the overarching tab in the top toolbar.
- Policy Management is also an **Application** in this case; a subsection of the Policy Management solution.
- The Exception Request **record** stores information pertaining to one exception. You can search for several records within an application.
- The Submitter **field** contains a specific piece of information relevant to the record.



# General Navigation

---



Now it's time to explore the interface components of the system.

# Login



- URL: <https://egrc.archer.rsa.com>

A screenshot of the RSA Archer eGRC User Login page. The page has a dark background with a light gray header and footer. The header contains the text "User Login". Below the header, there are three input fields labeled "User Name:", "Instance:", and "Password:". A "Login" button is positioned below the "Password" field. The footer contains the RSA Archer eGRC logo and the text "Powered by the RSA Archer eGRC Platform™".

The first step for working with the RSA Archer functions is to log in to the system.

To log in, you must have an active Archer user account set up by the Archer administrator. The user account includes your contact information, password and access rights within the system.

# RSA Archer Interface



The screenshot displays the RSA Archer interface for Policy Exception Management. The main content area features a 'Policy Exception Summary' dashboard with a bar chart showing 'Exceptions by Status' and a pie chart showing 'Exceptions Risk Overview'. The bar chart data is as follows:

Status	Count
In Review	12
Draft	4
Approved	4
Denied	2

The pie chart data is as follows:

Risk Rating	Count	Percentage
(No Selection)	13	59.09%
Low	3	13.64%
Medium Low	2	9.09%
Medium High	1	4.55%
High	2	9.09%
Not Rated	1	4.55%

The right-hand sidebar contains 'Policy Exception Quick Links', 'Confidentiality Statement', and 'GRC Contact Information'.

Once logged into Archer, you will notice the interface is divided up into a number of areas. Your view of the data may differ compared to what you see here, but the interface components will be the same.

The body of the interface is made up of one or more Workspace tabs. A Workspace is a tab and everything that falls below that tab, including the Navigation Menu and one or more Dashboards.

# RSA Archer Interface



The screenshot displays the RSA Archer interface for Policy Exception Management. The top navigation bar includes 'Administration', 'Enterprise Management', 'Incident Management', 'Risk Management', 'Policy Management', and 'Security'. The 'Dashboard' tab is selected. The main content area is titled 'Policy Exception Summary' and includes a description of the application. Below this are two overview sections: 'Exception Requests Overview' and 'Exceptions Risk Overview'. The 'Exception Requests Overview' section shows a bar chart with the following data:

Status	Count
In Review	12
Draft	4
Approved	4
Denied	2

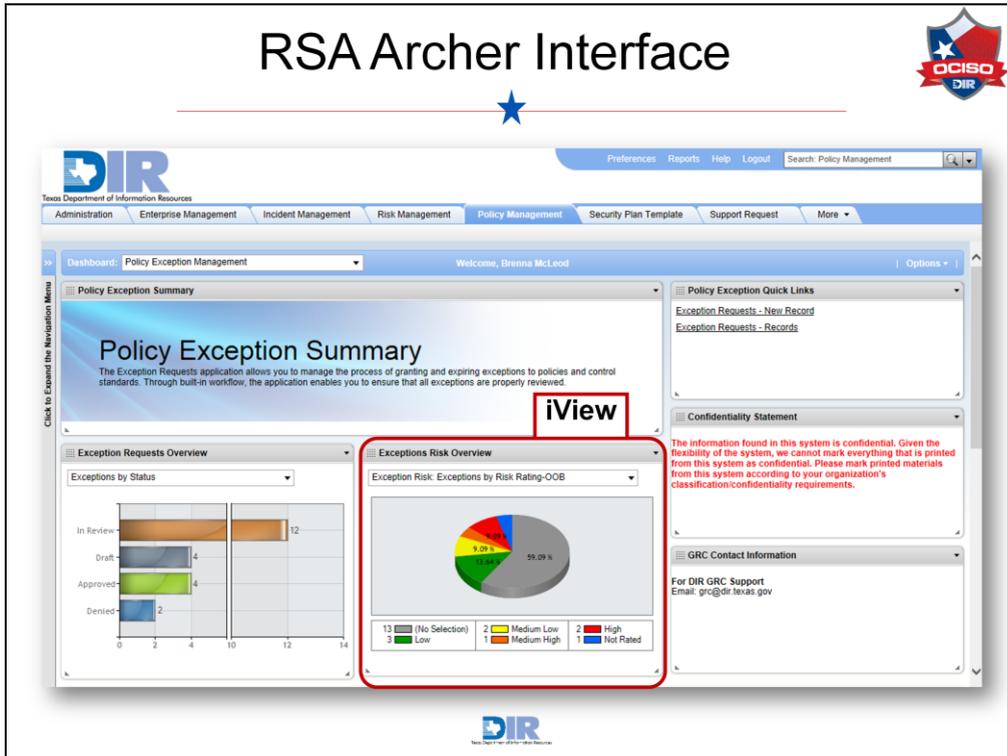
The 'Exceptions Risk Overview' section shows a pie chart with the following data:

Risk Rating	Count
(No Selection)	13
Low	3
Medium Low	2
Medium High	1
High	2
Not Rated	1

A red box highlights the main content area, and a red text box on the right side of the dashboard contains the following message: 'The information found in this system is confidential. Given the flexibility of the system, we cannot mark everything that is printed from this system as confidential. Please mark printed materials from this system according to your organization's classification/confidentiality requirements.'

A Workspace can contain one or more Dashboards, which are collections of windows that have been set up to display some kind of content. To switch between Dashboards on the same Workspace, use the Dashboard dropdown located at the top of the Workspace.

# RSA Archer Interface



The windows that comprise a Dashboard are called iViews. iViews most often are configured to display reports, but they can also display an embedded URL, custom content, videos, and other information as defined by the administrator. Each iView can be resized by a simple click-and-drag. The full version of a report shown within an iView can be accessed by clicking the small arrow in the upper right corner of the iView and selecting the *Display Report* option. To view other reports included within an iView, simply select the desired report from the dropdown menu at the top of the iView.

Take some time to explore the information displayed in the iViews you see when you log in. Links to actions like adding data or displaying records may be found, and you can click into any of the reports you see to access more information about the data comprising those reports. Dashboards and iViews are a great way to find quick links and relevant data. Becoming familiar with these screens will improve your overall Archer experience.

# RSA Archer Interface







Preferences Reports Help Logout Search: Policy Management

Incident Management Risk Management **Policy Management** Security Plan Template Support Request More

Dashboard: Policy Exception Management Welcome, Brenna McLeod Options

**Navigation Menu**

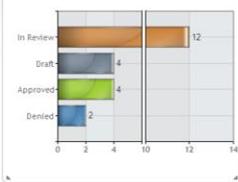
- Administration
- Policy Management
- Issue Management
- Findings
- Remediation Plans
- Exception Requests
  - Search Records
  - New Record
  - Records
    - By DIR Security Control Catalog
    - By Overall Status
    - By Reviewer
    - By Submitter
  - Reports

**Policy Exception Summary**

The Exception Requests application allows you to manage the process of granting and expiring exceptions to policies and control standards. Through built-in workflow, the application enables you to ensure that all exceptions are properly reviewed.

**Exception Requests Overview**

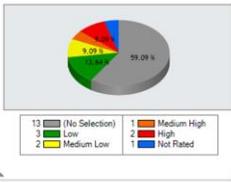
Exceptions by Status



Status	Count
In Review	12
Draft	4
Approved	4
Denied	2

**Exceptions Risk Overview**

Exception Risk: Exceptions by Risk Rating-OOB



Risk Rating	Count
No Selection	12
Low	3
Medium Low	2
Medium High	1
High	2
Not Rated	1

**Policy Exception Quick Links**

- Exception Requests - New Record
- Exception Requests - Records

**Confidentiality Statement**

The information found in this system is confidential. Given the flexibility of the system, we cannot mark everything that is printed from this system as confidential. Please mark printed materials from this system according to your organization's classification/confidentiality requirements.

**GRC Contact Information**

For DIR GRC Support  
Email: grc@dir.texas.gov

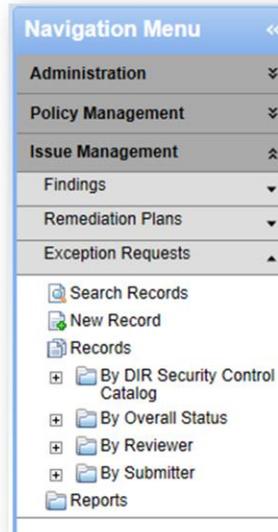


The collapsible Navigation Menu is another way to interact with data in Archer. Let's go to the next slide for further explanation.

# Navigation Menu Options



- Search for records
- Add a new record
- Display all records
- View filtered sets of records
- View reports



Unique to each Workspace, the navigation menu allows you to search for records, add new records, display records, and display reports. In this example, the user logged in can do a number of things within the Issue Management application, including searching for a record, adding a new record to the system, and displaying all of the Exception Requests records the user can access. Notice there is also the option to view records filtered by a number of different options, including by DIR Security Control Catalog, Overall Status, Reviewer, and Submitter. Clicking the Reports link will open a listing of all Exception Request-related reports that have been established in the system.



# Managing Content Records



Records are set up in a standardized format across Archer, regardless of how you're using the system. Let's take a look at how to work with these records.

# Accessing Content Records



The screenshot displays two windows from the 'Exception Requests' application. The top window shows a search results table with columns for Exception ID, Overall Status, Exception Description, DIR Security Control Catalog, and Submit Date. The bottom window shows the detailed view for Exception ID EXC-1, which is underlined in the top window. A red arrow points from the underlined 'EXC-1' to the detailed view window.

Exception ID	Overall Status	Exception Description	DIR Security Control Catalog	Submit Date
<u>EXC-1</u>	In Review	test	AC-01	11/20/2015
EXC-2	Approved	test		11/19/2015
EXC-3	Approved	test		11/19/2015
EXC-4	Denied	test description	AC-02	11/17/2015
EXC-5	Draft			
EXC-6	In Review			

**Exception Requests: EXC-1**

Date Created: 11/12/2015 7:32 AM Last Updated: 11/20/2015 11:06 AM

**General Information**

Exception ID:	EXC-1	Overall Status:	In Review
Submitter:	Thacker, Michelle	Organization:	
Submission Status:	Submit for Review	Submit Date:	11/20/2015
Requested Expiration Date:		Expiration Date:	
Reviewer:		History Log:	<a href="#">View History Log</a>



For this set of screenshots, we have chosen to display all Exception Request records that the user currently logged in can access. You'll see the Exception ID is underlined. When objects are listed on a page in underlined form, it indicates that the object name serves as a hyperlink to display additional information. In the example shown here, if we click on the Exception ID, the complete record for this exception would be opened to view the record's details.

# Record Toolbar Options



- New: Creates a new record
- Copy: Copies the record currently displayed
- Save: Saves your changes and closes the record
- Apply: Saves your changes and keeps the record open in Edit mode
- View: Takes you out of Edit mode and displays the record in View mode
- Edit: Opens the record for editing
- Delete: Permanently deletes the record



When you have a record open, you'll notice a toolbar that runs across the top of the record. One or more of these icons may be disabled based on your level of access. However, an explanation of each icon is as follows:

- New creates a new record.
- Copy creates a copy of the record you are currently viewing.
- Save saves any changes you have made to the record and closes the record. You will be taken back to the previously viewed page.
- Apply saves any changes you have made to the record, but leaves the record open in Edit mode so that you can continue working within the record.
- The View icon is only visible when you are working in Edit mode. Clicking View will take you to the read-only view of the record. This is often used to check formatting in text areas.
- The Edit icon is only visible when you are viewing the record in read-only view. Clicking Edit will open the record for editing.
- Delete deletes the record. You will first be prompted with a message confirming that you do want to delete the record. Once you delete a record, there is no way to undo the deletion. (Note: this icon is typically disabled for most users.)

# Record Toolbar Options



- Related: Displays the relationships between this record and other records
- Recalculate: Allows you to force the recalculation of all fields within the record.
- Export: Exports the record into a number of formats (.doc, .xls, .pdf, etc.)
- Print: Opens a print preview window and prompts you to print the record
- Email: Opens a new email message in your default email client with a deeplink to the record.
- X icon: Closes the current screen and returns you to the previous screen



On the right side of the toolbar, we have these icons:

- The Related icon opens a relationship visualization showing related records and applications. From here you can see displayed fields of the record, and jump to any record associated to it.
- The Recalculate button refreshes the fields so any fields capturing calculations are up to date.
- You may click the Export icon to export a record to a number of different formats (Rich Text, Excel, PDF, etc.) Clicking this icon will prompt you to select a format and the record will subsequently be exported. This is often used if you need to save a record to send via email to someone who does not have Archer access.
- Upon clicking the Print icon, a Print Preview window will open from which you may print the record.
- The Email icon will prompt a new email message to be created in your default email program. The new email message will include a link to the record you are currently viewing. The recipient of the email will have to login to Archer in order to view the record you have linked via email.
- The Question Mark icon opens context-sensitive help that will remind you of your options on this screen.
- The X icon will close you out of the record and return you to the previously viewed screen. Use of this icon will NOT save any changes you have made to the record.

# Saving Your Work



- When in doubt, click Apply often
- Click Save when done with the current screen
- If you close the browser or click the , any unsaved changes are lost
- No warning is given if you navigate away from unsaved changes



It is essential that we call out the importance of manually saving your work. The RSA Archer system will not automatically or periodically save your data. As you make changes to records, be sure to click Apply to save and continue working, or click Save to save and close the record. This is true of all areas of Archer. If you navigate away from a screen on which you have made changes, no warning message or prompt is given for you to save your changes.



# Policy Management

Part One

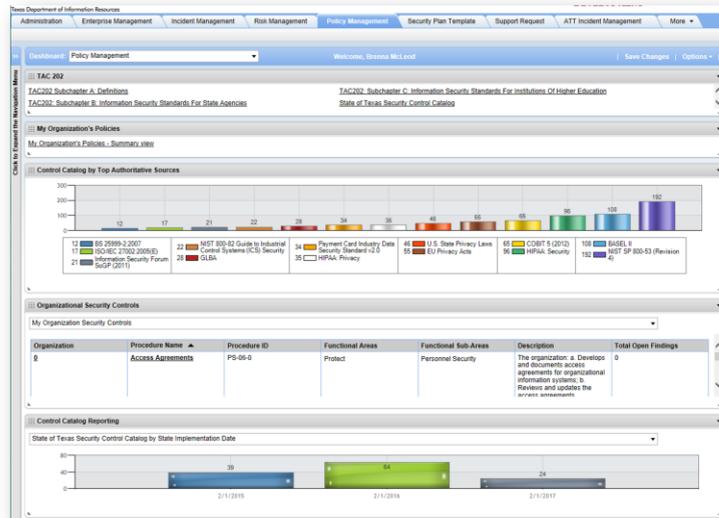


Let's move into the Policy Management section of Archer.

# Policy Management Dashboard



- TAC 202
- My Organization's Policies
- Control Catalog by Top Authoritative Sources
- Organizational Security Controls
- Control Catalog Reporting



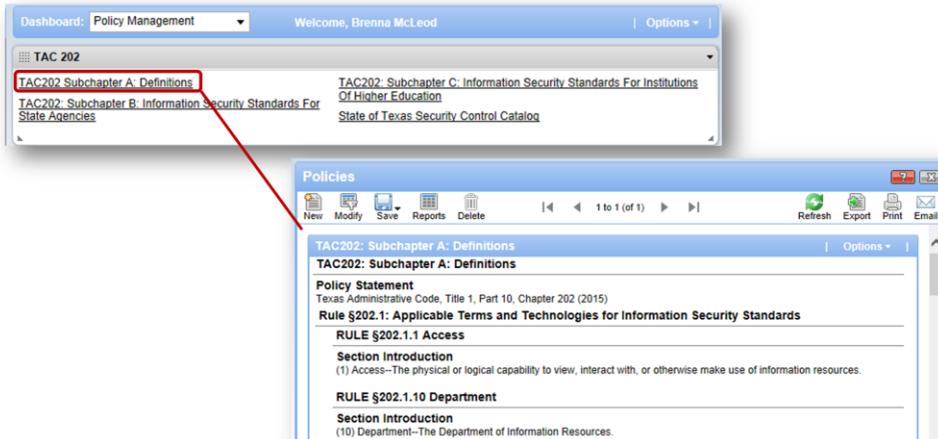
Within the Policy Management workspace, you can switch from the Policy Exception dashboard to the Policy Management dashboard by using the dropdown menu at the top. In this dashboard, you can see the TAC 202 policies and your organization's policies. There are also iViews on the Control Catalog by Top Authoritative Sources, Organizational Security Controls, and Control Catalog Reporting.

Let's start by examining TAC 202 policies in this Policy Management workspace.

# TAC 202 Policies



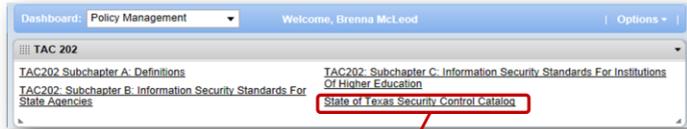
- View TAC 202 policies through dashboard



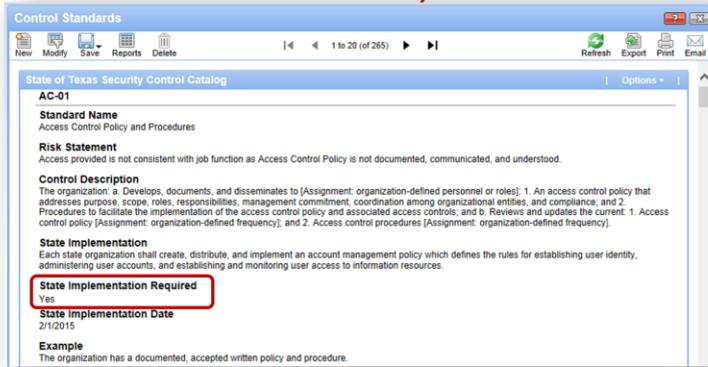
By default, the only policies available are those pertaining to TAC 202, but you do have the option to add your own policies, which we'll see momentarily. These screenshots display what opens when clicking on a TAC 202 policy from the dashboard iView.

Notice it is set up in an outline format, with the policy statement at the top, followed by indented sections and areas. These policies are here for your reference and can be accessed at any time.

# State of Texas Security Control Catalog



- View the 265 Controls adopted by the state of Texas
- Not every organization uses all Controls



Also from the TAC 202 iView, you can access the State of Texas Security Control Catalog. The state of Texas has adopted 265 NIST 800-53 controls, which are all listed in the system, but not every organization uses all of the controls. You can see if the control is state-mandated from this view, as well as the Description, State Implementation Date, and an example.



# Creating Policies

---

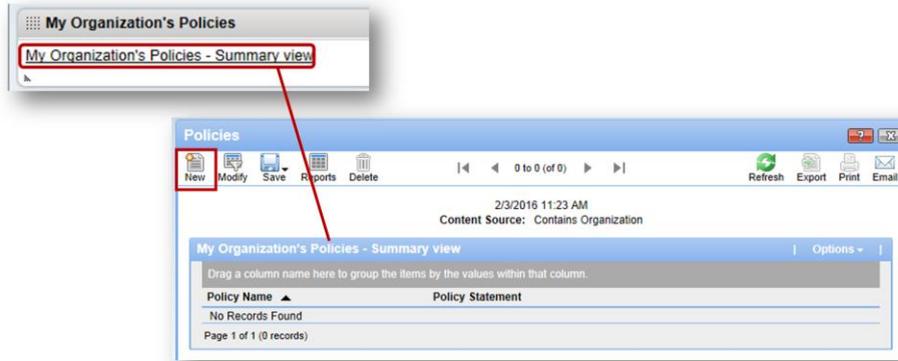


Let's look at creating new Policies.

# My Organization's Policies



- View your organization's policies
- The Security Office and IRM can create new policies



From the dashboard, there is the option to open *My Organization's Policies*. Clicking that link opens a summary view of any policies created specifically for your organization. Only the Security Office and IRM roles can create new policies in the system, and they'll begin by selecting the New icon.

# Creating a Policy



- Select the Policy data level and click Continue

A screenshot of a software dialog box titled "Add New Record". The dialog box has a blue header bar with the title and a close button. Below the header, there is an information icon and the text "Please select the data level where you want to create a new record". There are three radio button options: "Policy", "Area", and "Section". Each option is followed by a detailed description of that level. The "Policy" option is selected. At the bottom right of the dialog box, there is a "Continue" button.

**Add New Record**

Please select the data level where you want to create a new record

**Policy** A Policy is a broad statement of principle that presents management's position for a defined area. Policies are intended to be long-term and guide the development of more specific rules to address specific situations. Policies are interpreted and supported by standards, baselines and procedures. Policies should be relatively few in number; must be approved and supported by executive-level management, and must provide overall direction to the organization. For ease of communication to employees of the firm, a three-level policy structure has been designed. The intent of this structure is to allow employees to quickly locate policies based on a high-level name, an area of focus or a specific section. A Policy name is the highest-level item in the Policy Framework. Policy names include high-level statements of management expectations regarding a security issue (e.g., 8.0 Access Control).

**Area** An Area is the second highest level in the Policy Framework. Areas include more specific language regarding the policy, describing an area of focus of the main level policy and its intent. Areas act as a categorical stepping-stone to help users navigate to the sections they are looking for (e.g., 7.1 User Access Management).

**Section** A Section is the third level of policy in the Policy Framework. Sections provide an additional level of grouping (e.g., 7.1.5 Password Composition).

Continue

\*New Policies or Control Procedures will *not* be automatically linked to Risk Assessments



The first window to open will ask you to select the data level of the new policy: either Policy, Area, or Section. Policies often come from a long Word document, broken up by areas and sections. Recall policies in the system are also displayed in an outline format, so this selection essentially tells the system where in the outline this piece of information belongs. Keep your original document in mind when converting it to records in the system.

Information about each level is provided in the window. At a high level, policies are the broad principle statement, areas describe an area of focus for the policy, and sections provide an additional level of grouping. Click Continue once the correct level is selected.

It is also important to note at this stage that new Policies or Control Procedures will not be automatically mapped or linked to Risk Assessments.

# General tab



• Identify a unique numbering or labeling system for your organization

• Paste data from your original document into the Policy Statement and Purpose fields

For training purposes, we are looking at a complete policy, but when you create a new policy record, each of these fields will be blank.

Begin with the General tab:

- Create a **Policy Name** and **ID**. Here is where DIR asks you to come up with a unique labeling system for your organization, including adding your agency number to the end of these fields. In this example, the Organization Number is 0. Both the Policy Name and Policy ID is followed by a dash and a zero. DIR asks you to identify your organization so that user access rights are appropriately assigned and so that policy names and IDs are unique to your organization.
- The **Status** field will be updated as the policy goes through different stages: Under Review, Published, or Retired.
- Select the policy **Domain** by clicking the ellipsis button to open a values popup.
- Provide a **Policy Statement** and **Purpose**. This is where you can likely copy and paste the information from a portion of your original policy document.

There are a few more fields in the Policy section that we will explore on the next slide.

## General tab, cont.



- Complete the Policy information section and move into the Policy Management tab



Continuing through the Policy section:

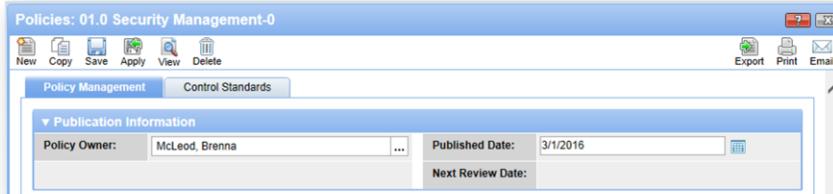
- Provide a **Policy Scope**.
- Identify the **Areas of Reference** and your **Organization** number.

Below this Policy section are tabs on Policy Management and Control Standards. We'll look at those next.

# Policy Management sub-tab



- Complete Publication Information



The Policy Management tab displays the Policy Owner and Published Date. Policies that have been previously built into the system will not designate a Policy Owner or Publish date.

# Control Standards sub-tab



The screenshot shows the 'Policies: 01.0 Security Management-0' application window. The 'Control Standards' sub-tab is active, displaying a table with columns for Standard ID, Standard Name, Grouping, and Classification. A 'Lookup' button is highlighted with a red box. Below it, the 'Record Lookup' dialog box is open, showing a table of control standards with checkboxes for selection. The 'ATCS-065' row is selected. The 'OK' button is also highlighted with a red box.

Standard ID	Standard Name	Grouping	Classification	
<input type="checkbox"/>	ATCS-346	Acceptable Use of Modems	Remote Environments Security Assessment and Authorization	Preventive
<input checked="" type="checkbox"/>	ATCS-065	Acceptable Use Policy (AUP)	Personnel Security	Preventive
<input type="checkbox"/>	ATCS-1183	Acceptance of Deposits by Proprietorship Concerns/Firms/Companies in India on Non-Repatriation Basis	Financial Services Legal and Regulatory Compliance	Preventive
<input type="checkbox"/>	ATCS-541	Acceptance of Facilities	Application Development External Supplier Information Risk Service Level Agreements System Development Methodology	Preventive

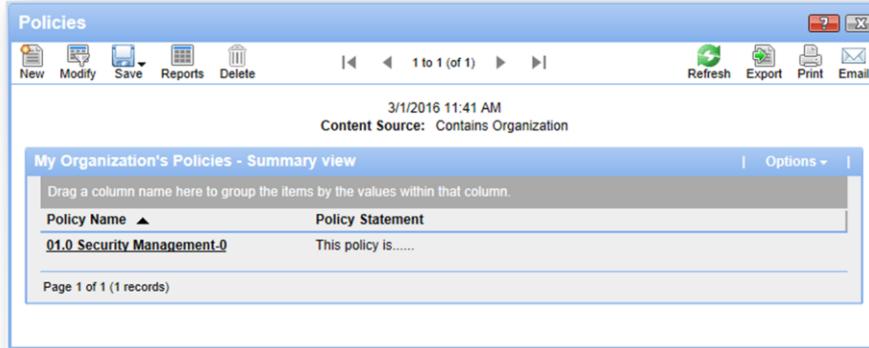
- Click the *Lookup* link to associate related NIST Control Standards to the Policy

The Control Standards tab provides a place to link this Policy to NIST Control Standards from the system library. Click the Lookup link and check the box next to the relevant Control Standards. Click OK to associate them to the record.

# View Your Complete Policy



- Save and close the record once complete
- Repeat these steps until your full policy is in the system



Once your Policy record is complete, click the Save icon to return to your organization's policies. You should see the new policy in your Summary View. Continue adding records until your full policy is in the system.

Let's take a quick look at a Policy Area record. Click the New icon again to create another record.

# Creating a Policy Area



- Select the Area level

A screenshot of a software dialog box titled "Add New Record". The dialog has a blue header bar with the title and a close button. Below the header is an information icon and the text "Please select the data level where you want to create a new record". There are three radio button options: "Policy", "Area", and "Section". The "Area" option is selected. Each option is followed by a descriptive paragraph. At the bottom right of the dialog is a "Continue" button.

**Add New Record**

Please select the data level where you want to create a new record

**Policy** A Policy is a broad statement of principle that presents management's position for a defined area. Policies are intended to be long-term and guide the development of more specific rules to address specific situations. Policies are interpreted and supported by standards, baselines and procedures. Policies should be relatively few in number, must be approved and supported by executive-level management, and must provide overall direction to the organization. For ease of communication to employees of the firm, a three-level policy structure has been designed. The intent of this structure is to allow employees to quickly locate policies based on a high-level name, an area of focus or a specific section. A Policy name is the highest-level item in the Policy Framework. Policy names include high-level statements of management expectations regarding a security issue (e.g., 8.0 Access Control).

**Area** An Area is the second highest level in the Policy Framework. Areas include more specific language regarding the policy, describing an area of focus of the main level policy and its intent. Areas act as a categorical stepping-stone to help users navigate to the sections they are looking for (e.g., 7.1 User Access Management).

**Section** A Section is the third level of policy in the Policy Framework. Sections provide an additional level of grouping (e.g., 7.1.5 Password Composition).

Continue



To create an Area record, select the Area level from the window and click Continue.

# Policy Area General Information



Area Name:	01.1 Security Area-0 Updated by McLeod, Brenna on 3/1/2016 11:54:37 AM	Area ID:	SA-001-0 Updated by McLeod, Brenna on 3/1/2016 11:54:37 AM
Area Statement:	This Area...		
Area Introduction:			
Policy Reference (s):	01.0 Security Management-0	Section Reference(s):	
Area Access History:	<a href="#">View Access History</a>		

Standard Name	Grouping	Classification
No Records Found		

- Use the same organization identifier when providing the Area Name and ID
- Associate a Policy record
- Add NIST Control Standards

In the Policy Area record:

- Add an **Area Name** and **ID** using the same unique labeling chosen for the policy record.
- Provide the **Area Statement** and **Introduction** – likely more pasted information from your document.
- Identify the **Policy Reference** which is where the Area will belong. You will also see referenced Sections in this area once they are associated.
- The section on Control Standards works the same way as in the Policy record – click the Lookup link to associate the Area to NIST standards.

When the information is complete, click the Save icon to return to your Organization's Policies.

# View Your Complete Area



- Your complete Area record will appear in your Policy record in the Area References field

The screenshot shows a web application window titled "Policies: 01.0 Security Management-0". The interface includes a menu bar with options like New, Copy, Save, Apply, Edit, Delete, Related, Recalculate, Export, Print, and Email. Below the menu bar, there is a "General" tab and an "About" section. The "Policy" section contains the following fields:

Policy Name:	01.0 Security Management-0	Policy ID:	0-001
Status:	Published	Domain:	
Policy Statement:	This policy is.....		
Policy Purpose:			
Policy Scope:	This policy covers....		
Area Reference(s):	01.1 Security Area-0 1. Section Policy	Organization:	0

The "Area Reference(s)" field is highlighted with a red border.



Click into your policy and view your complete Area record in the Area References field. Click the New icon to create another record; we'll look at a Section record next.

# Creating a Policy Section



Policies: Add New Record

General Reference Content

About

Section

Section Name: 01.1.1 Security Section-0 Section ID: SS-001-1-0

Section Introduction: The Section...

Area Reference: 01.1 Security Area-0 Add

Section Access History: View Access History

Control Standards

Control Standards | Add New | Lookup

Standard Name	Grouping	Classification
No Records Found		

- Select the Section level and complete the Section information
- Identify the Area Reference and NIST Controls Standards

Creating a Section is similar to creating an Area: select the Section level from the first window, and complete the Section information. Again, be sure to include your organization's labeling system in the Section Name and ID. Associate the Area where this section belongs, and any related NIST Control Standards. Save the record and click into the associated Area record.

# View Your Complete Section



- Your complete Section record will appear in the Area record in the Section Reference field

The screenshot shows a software interface for managing policies. The title bar reads "Policies: 01.1 Security Area-0". Below the title bar is a menu bar with options: New, Copy, Save, Apply, Edit, Delete, Related, Recalculate, Export, Print, and Email. There are two tabs: "General" and "Reference Content". Under the "Reference Content" tab, there is a section titled "About" with a dropdown arrow. Below "About" is a section titled "Area" with a dropdown arrow. The "Area" section contains the following fields:

Area Name:	01.1 Security Area-0	Area ID:	SA-001-0
Area Statement:	This Area...		
Area Introduction:			
Policy Reference (s)::	01.0 Security Management-0	Section Reference(s)::	01.1.1 Security Section-0

The "Section Reference(s)::" field is highlighted with a red border.

- Repeat these steps until your full policy in the system.



Your complete Section record will appear in the Area record in the Section Reference field. Repeat these steps until your full policy is recorded in the system.



# Policy Management

---

★  
Part Two



Let's return to the Policy Management workspace to explore the remaining iViews.

# Authoritative Sources



The screenshot displays the Archer system interface. At the top, there are navigation tabs: Risk Management, Policy Management, Security Plan Template, Support Request, and More. A star icon is positioned above the tabs. On the left, a vertical navigation menu is visible with a red box around the 'Control Catalog by Top Authoritative Sources' link and a red arrow pointing to it. The main area shows a bar chart with the following data series:

Source ID	Source Name	Count
12	BS 25999-2:2007	12
17	ISO/IEC 27002:2005(E)	17
21	Information Security Forum SoGP (2011)	21
22	NIST 800-82 Guide to Industrial Control Systems (ICS) Security	22
28	GLBA	28
34	Payment Card Industry Data Security Standard v2.0	34
35	HIPAA: Privacy	35
46	U.S. State Privacy Laws	46
55	EU Privacy Acts	55
65	COBIT 5 (2012)	65
96	HIPAA: Security	96
108	BASEL II	108
192	NIST SP 800-53 (Revision 4)	192

Below the chart is a legend with colored boxes corresponding to the bars. A red box highlights the '96' value for 'HIPAA: Security', with a red arrow pointing to it. Below the chart is a detailed view window titled 'Authoritative Sources' showing search results for 'HIPAA: Security'. The table below is a reproduction of the data shown in this window:

Source Name	Standard ID	Risk Statement
<b>HIPAA: Security</b>		
Law/Regulation		
Access Control Policy and Procedures	AC-01	Access provided is not consistent with job function as Access Control Policy is not documented, communicated, and understood.
Account Management	AC-02	Unauthorized access is gained to information systems.
Access Enforcement	AC-03	Misconfigured access controls provide unauthorized access to information held in application systems.
Information Flow Enforcement	AC-04	Users gain access to information that is beyond their appropriate level of privilege.
Separation of Duties	AC-05	The lack of user segregation of duties may result in unauthorized or unintentional modification or misuse of the organization's information assets.

- View Controls by Authoritative Source

- Click the data in the graph to open a detailed list of Controls

Here, we've gone back to the Policy Management Dashboard. Under My Organization's Policies is a graph on the Control Catalog by Top Authoritative Sources. Authoritative Sources in Archer are the governed documentation requiring specific actions be taken by organizations: NIST, HIPAA, U.S State Privacy Laws, EU Privacy Acts, and more are listed.

Here, you can see 192 Controls are related to NIST, 108 are related to BASEL II, 96 are related to HIPAA: Security, and so on. This is another reference item for you. If you need to see all controls related to the Security side of HIPAA, you can click the green bar to open a record listing of those 96 control records.

Note Authoritative Sources are also accessible through the Navigation Menu on the left side of the screen. Recall you can expand the Menu using the arrows at the top.

# Organizational Security Controls



Organization	Procedure Name	Procedure ID	Functional Areas	Functional Sub-Areas	Description	Total Open Findings
0	Access Agreements	PS_06_0	Protect	Personnel Security	The organization: a. Develops and documents access agreements for organizational information systems; b. Reviews and updates the access agreements (assignment, organization-defined frequency); and c. Ensures that individuals requiring access to organizational information and information systems:	0

- DIR has copied the 265 Controls in the State Catalog for each organization
- Select different Controls filters from the dropdown menu



The next piece of the dashboard provides a look at your Organization's Security Controls. DIR has copied the 265 controls from the state catalog, and made them specific to each organization so the Security Office and IRM can edit each control to better suit it to your organization. We'll look at a specific example in a moment.

The default display shows the full list of Controls, but you can switch views using the dropdown menu. Other options include your organization's Security Controls Tied to Key Controls, Controls by Total Open Findings, and Controls by Functional Area.

# Control Procedures



The screenshot shows the Archer system interface. At the top, there are navigation tabs: Risk Management, Policy Management, Security Plan Template, Support Request, ATT Incident Management, IRDR, and More. Below this is a table titled "My Organization Security Controls". The table has columns for Organization, Procedure Name, Procedure ID, Functional Areas, Functional Sub-Areas, Description, and Total Open Findings. The first row is highlighted, with a red box around the Procedure ID "PS-06-0" and a red arrow pointing to it. To the right of the table, there are two bullet points: "Click the Procedure ID to open a Control record" and "Security Office and IRM can edit Control Procedure records". Below the table, a window titled "Control Procedures: PS-06-0" is open, showing a detailed view of the control procedure. The window has a menu bar with options: New, Copy, Save, Apply, Edit, Delete, Related, Recalculate, Export, Print, and Email. The main content area is divided into sections: "About", "General Information", and "Risk Statement". The "General Information" section contains the following data:

Procedure ID:	PS-06-0	Organization:	0
Procedure Name:	Access Agreements	Status:	Active
Description:	The organization: a. Develops and documents access agreements for organizational information systems; b. Reviews and updates the access agreements [Assignment: organization-defined frequency]; and c. Ensures that individuals requiring access to organizational information and information systems: 1. Sign appropriate access agreements prior to being granted access; and 2. Re-sign access agreements to maintain access to organizational information systems when access agreements have been updated or [Assignment: organization-defined frequency].		
Risk Statement:	Employees or contractors do not agree or sign terms or conditions of employment.		

These organization-specific Security Controls are labeled as Control Procedures in Archer. When you select a Control from the dashboard, you will see the full record open up, giving you general information, implementation steps and dates, and Findings linked to the Control. Also notice the Procedure ID here includes the Organization Number. Let's look at what you can edit in a Control Procedure.

Each organization can modify the standard to make it even more stringent and put in their own effective dates or specific steps. Both the ISO and IRM roles can create and edit procedures within the Control Procedures application. All other users have access to view them. Over the next few slides, we'll outline how to create a Control Procedure, and how to create Findings and Exceptions from within a Control Procedure.

To create a new Control Procedure, you can click New Record in the Navigation Menu, or the New icon from the Records view of Control Procedures.

## Editing Control Procedures – General Information



- No fields in the of the General Information can be edited

The screenshot shows a web application window titled "Control Procedures: PS-06-0". The interface includes a menu bar with options: New, Copy, Save, Apply, View, Delete, Export, Print, and Email. The main content area is titled "General Information" and contains the following details:

<b>Procedure ID:</b>	PS-06-0 Updated by Golka, Jean on 12/14/2015 3:29:13 PM	<b>Organization:</b>	0
<b>Procedure Name:</b>	Access Agreements	<b>Status:</b>	Active
<b>Description:</b>	The organization: a. Develops and documents access agreements for organizational information systems; b. Reviews and updates the access agreements [Assignment: organization-defined frequency]; and c. Ensures that individuals requiring access to organizational information and information systems: 1. Sign appropriate access agreements prior to being granted access; and 2. Re-sign access agreements to maintain access to organizational information systems when access agreements have been updated or [Assignment: organization-defined frequency].		
<b>Risk Statement:</b>	Employees or contractors do not agree or sign terms or conditions of employment.		



Once you click the Edit icon, you'll notice the General Information section remains in read-only view, but let's take a look at Implementation.

# Editing Control Procedures – Implementation



• Identify an earlier Implementation Date if desired

• Copy and Paste the Description to edit Organization Assignments

In the Implementation section, you will see fields regarding both State and Organization-specific implementation. When we look at creating Control Procedures from scratch, you will not see the State Implementation fields. Here, you can edit the Procedure to fit your organization’s requirements.

- First, indicate whether the control is required by your organization.
- Then, select an Organization Implementation Date. The State Implementation Date here is February 1, 2017, but if your organization wants to have this control implemented by October 1, 2016, you can set a more stringent target date.
- Provide Organization Implementation details. A lot of the time, the Control Description in the General Information section will have specified Assignments for the organization. In this Control, each organization needs to define the frequency with which they will update access agreements. Since that field is read-only, you can copy and paste the text from the Description into the Organization Implementation text box and edit the assignments.
- Finally, update the Testing Procedures if your organization plans to follow different steps than those already listed.

## Editing Control Procedures – Findings and Exceptions



- Click the *Lookup* link to identify other Findings
- Add or look up an Exception Request if a Control cannot be implemented

The screenshot shows a web application window titled "Control Procedures: PS-06-0". The interface is divided into several sections:

- Statistics:** A summary table showing:

Total Open Findings:	0	Total All Findings:	1
Number of Assessments:	<input type="text"/>	Total Exceptions:	0
- Findings:** A table with columns: Finding ID, Finding, Target, and Status. A "Lookup" link is highlighted in a red box.

Finding ID	Finding	Target	Status
FND-48	The question: "Do you have documented personnel security requirements for third party providers (e.g. requirements on background checks and other screening/training requirements, etc.) and are there processes in place to monitor their compliance to such requirements (e.g. sample checks by the organization and / or third-party assessment reports)?" was answered incorrectly. Question: NIST-R0123-PS-07 Answer: Partially implemented Question Risk Score: 0.5	Organization @	Risk Accepted
- Exceptions:** A table with columns: Exception ID, Organization, and Purpose. A "Lookup" link is highlighted in a red box.

Exception ID	Organization	Purpose
No Records Found		



Below the Implementation section are sections on Findings, Finding Statistics, and Exceptions. In the Findings Statistics section, you can view the Total Open Findings, Total of all Findings – whether open or closed, Total Exceptions, and the Number of Assessments. These statistics are populated based on the associated Control Standards in the Control Catalog and Key Controls tab. You can manually edit the Number of Assessments, but all other fields are not editable.

Findings are created when Control Assessments are completed on the associated Control Standards, and will appear in the Procedure in this Findings section. If you know the Control Procedure should have a specific Finding associated to it, click the *Lookup* link to find the appropriate Finding.

The Exceptions section exists for the cases in which a Control cannot be implemented. You can add an exception, or look up an existing one. Please refer to the Policy Exception Management section of this training for details on exception requests.

# Editing Control Procedures – Key Controls



- Identify further Key Controls, Control Standards, and NIST reference data

The screenshot shows a software interface titled "Control Procedures: PS-06-0". It has a menu bar with options: New, Copy, Save, Apply, View, Delete, Export, Print, Email. Below the menu bar are two tabs: "Findings and Exception Requests" and "Control Catalog / Key Controls".

The "Control Catalog / Key Controls" tab is active and contains three main sections:

- Security Plan Template Key Controls**: A table with columns: Tracking ID, Organization Name, Functional Area, Security Objective, End Date. One row is visible: Tracking ID 233255, Organization Name State Agency for Archer, Functional Area Protect, Security Objective Personnel Security.
- Control Standards**: A table with columns: Standard ID, Standard Name, Risk Statement. One row is visible: Standard ID PS-06, Standard Name Access Agreements, Risk Statement Employees or contractors do not agree or sign terms or conditions of employment.
- NIST**: A form with fields: Functional Areas (Protect), Functional Sub-Areas (Personnel Security), NIST Requirement (R0149), and Category (Personnel Security).



The Control Catalog and Key Controls sub-tab is another area of reference for you. You can see which Security Plan Template Key Controls and Control Standards are associated to the Control Procedure, and which areas it satisfies under NIST. The assessments completed to evaluate the Control Standards can be found by clicking into the Control Standard record. You have the option to look up further Key Controls and Control Standards to relate to this Control Procedure.

In the NIST section, you can populate the fields based on which categories in the security plan template the procedure addresses. In this example, our procedure on access agreements falls under the Protect Functional Area, and is related to Personnel Security in the Functional Sub-Area. The specific NIST Requirement can also be provided.

# View Your Updated Procedure



- Save all of your changes
- Return to the same record to review the updates

Control Procedures: PS-06-0

New Copy Save Apply Edit Delete Related Recalculate Export Print Email

**General Information**

Procedure ID:	PS-06-0	Organization:	Q
Procedure Name:	Access Agreements	Status:	Active
Description:	The organization: a. Develops and documents access agreements for organizational information systems; b. Reviews and updates the access agreements [Assignment: organization-defined frequency]; and c. Ensures that individuals requiring access to organizational information and information systems: 1. Sign appropriate access agreements prior to being granted access, and 2. Re-sign access agreements to maintain access to organizational information systems when access agreements have been updated or [Assignment: organization-defined frequency].		
Risk Statement:	Employees or contractors do not agree or sign terms or conditions of employment.		

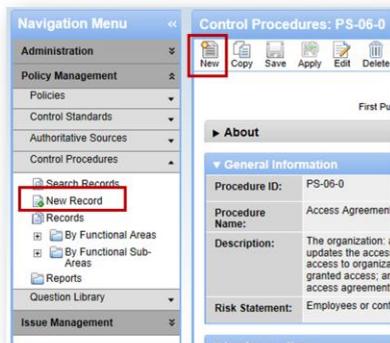
**Implementation**

State Implementation Required:	Yes	State Implementation Date:	2/1/2017
State Implementation:	The state organization completes appropriate signed access agreements for individuals requiring access to organizational information and information systems before authorizing access.		
Example:	Employees sign access agreements.		



When your Control Procedure record is complete, be sure to save your changes. Return to the same record to ensure the updates you made have been properly recorded.

# New Control Procedures



- The Security Office or IRM can create Control Procedures
- Click the New icon from an existing record, or expand the Navigation Menu and select to add a new Control Procedure
- Creating new Procedures will look similar to editing them, but more fields are available

\*New Control Procedures will not be automatically linked to Risk Assessments.



Now let's take a look at creating Control Procedures. The Security Office or IRM roles can create Control Procedures by either clicking on the New icon from an existing Procedure, or going through the Navigation Menu. Creating new Procedures will look similar to editing them, but more fields are available for you to manually add information. We'll go through those fields next.

Please remember that new Control Procedures will not be automatically linked to Risk Assessments.

# Creating a Control Procedure



Control Procedures: Add New Record

New Copy Save Apply View Delete

General Information

\* Procedure ID: i.e. AC-01-101 (organization number)

\* Procedure Name:

- Add your organization's number to Procedure ID

- Provide a Description and Risk Statement if applicable

Control Procedures: Add New Record

New Copy Save Apply View Delete Print Email

General Information

\* Procedure ID: CIS-101-0 \* Organization: 0 Add

\* Procedure Name: Install the latest software version of ABC. \* Status: Active Edit

\* Description: Ensure the newest version of ABC is installed to fix bugs and guard against security issues.

Risk Statement:

Implementation



When creating a Control Procedure there are a number of required fields to complete, denoted by the red asterisk. Different from editing an existing Procedure, you now have influence over the General Information section. Begin by creating a Procedure ID. When you first open the new record, you will see an ID example that reminds you to include your organization's number.

Next, identify your Organization and give your procedure a Name and Description. The Status can either be *Active* or *Inactive*. Procedures currently in use should remain in *Active* status.

The last field in the General Information section calls for a Risk Statement. It is optional, but if your procedures yield any kind of risk to the organization, it will benefit you to explain potential threats.

# Creating a Procedure – Implementation



- Only the Organization Implementation information appears in new Procedures

A screenshot of a web application window titled "Control Procedures: Add New Record". The window has a menu bar with "New", "Copy", "Save", "Apply", "View", and "Delete". On the right side of the menu bar are "Print" and "Email" icons. Below the menu bar is a section titled "Implementation". This section contains two input fields: "Organization Implementation Required:" and "Organization Implementation Date:". Below these fields is a large text area labeled "Organization Implementation:". At the bottom of the form is another large text area labeled "Testing Procedures:". The DIR logo is visible at the bottom center of the window.

As previously mentioned, when creating a Control Procedure, you will only see the Organization's implementation information here – the state information is only added to procedures adopted by the state.

# Creating a Procedure – Sub-tabs



- View Statistics and Findings based on the Control Standard Risk Assessments

- Add related Key Controls, Control Standards, and NIST information



The same fields are available for editing in these final sub-tabs. Again, the Statistics and Findings are pulled from the assessments completed on referenced Control Standards.

The same information previously explored can also be provided in the Control Catalog and Key Controls sub-tab.

# View Your New Procedure



- Save your record and return to the dashboard
- Confirm your new Control Procedure is listed with your other Organizational Security Controls

Organization	Procedure Name ▲	Procedure ID	Functional Areas	Functional Sub-Areas	Description	Total Open Findings
g	Access Agreements	PS-06-0	Protect	Personnel Security	The organization: a. Develops and documents access agreements for organizational information systems; b. Reviews and updates the access agreements [Assignment: organization-defined frequency]; and c. Ensures that individuals requiring access to organizational information and information systems: 1. Sign appropriate access agreements prior to being granted access; and 2. Re-sign access agreements to maintain access to organizational information	0



When your record is complete, save the changes and return to the My Organizational Security Controls iView on the dashboard. Confirm your new Control Procedure is included in this section.



# Policy Exception Management

---



Let's take a look at the Policy Exception Management dashboard.

# Policy Exception Dashboard



- Policy Exception Quick Links
- Exception Requests Overview
- Exceptions Risk Overview
- My Policy Exception Requests
- Exception Status

Still within the Policy Management workspace, you can click the dropdown menu at the top of the page to switch to the Policy Exception dashboard. On this dashboard, you will see a number of useful iViews. The Policy Exception Summary gives you a brief statement on the application's purpose. You can use the Policy Exception Quick Links to be taken directly to the full list of exception requests or to a new exception request record.

The Exception Requests Overview iView displays reports of the filter described in the dropdown menu. You can access the data in these reports by clicking the bars. The My Policy Exception Requests iView displays the exceptions you have submitted. The Exception Status iView displays the Exceptions according to the filter specified in the dropdown menu.

# Exception Request Record



- Complete General Information and Purpose sections

General Information		Overall Status:	
Exception ID:		Organization:	0
Submitter:	McLeod, Brenna	Submit Date:	3/1/2016
Submission Status:	Draft	Expiration Date:	
Requested Expiration Date:	12/30/2016	History Log:	<a href="#">View History Log</a>
Reviewer:	Doe, John		

Purpose	
DIR Security Control Catalog:	AC-01
Organizational Control Catalog:	ATCP-26850

Finding ID	Finding	Target	Status	Category	Control Procedures	Control Standards
No Records Found						



Almost every user can create Exception Requests, but only the identified reviewer, ISO, and IRM can approve the exceptions. Most users will need to go through the Policy Exception Management Workspace just shown, though users on the Security Office team or IRM can add Exceptions directly from a Control Procedure. Whichever way you add the Exception, it will look like the record on the screen.

You can begin in the General Information section:

- Identify the **Submitter** if your name does not already appear in the field.
- Provide your **Organization** number.
- Update the **Submission Status** and **Submit Date** as needed.
- The **Requested Expiration Date** will be populated by the Submitter. When the Reviewer looks over the record, they will submit a final **Expiration Date** that may or may not be the same as the Requested Date. Emails will be sent to the submitter when an exception is approaching its expiration date.
- Identify a **Reviewer** to review and approve the record. The Reviewer may be any user in the system; it's not limited to the ISO or IRM. When the record is complete and ready for review, the Reviewer will receive a notification.

There are a few fields left to complete in the Purpose section.

- The **DIR Security Control Catalog** field may auto-populate based on where you

created the exception. If it is not already populated, click the ellipsis button to select the DIR Control.

- Do the same for the **Organizational Control Catalog** as necessary.
- Attach any **Findings** related to these Controls.

Be sure to click Apply often to save your work and remain on the same page.

# Exception Declaration



- Provide an Exception Description and Business Justification at minimum

A screenshot of a web application window titled "Exception Requests: Add New Record". The window has a menu bar with "New", "Copy", "Save", "Apply", "View", and "Delete" options, and "Print" and "Email" buttons. Below the menu bar is a section titled "Exception Declaration" with a dropdown arrow. It contains three text input fields:

- Exception Description:** "Enter a description of the exception." The input field contains the text "Too difficult to carry out..."
- Business Justification:** "Provide a business justification or rationale for the exception request." The input field contains the text "Would be too costly..."
- Business Impact:** "Describe the business impact if an exception request is not granted." The input field contains the text "Minimal impact to the business..."



The next section covers the Exception Declaration. Provide a **Description** of the Exception, the **Business Justification** for accepting the risk, and what **Impact** the exception might have on the business. Note the Exception Description and Business Justification are required fields, while the Business Impact is optional.

# Compensating Controls



- Identify any compensating controls
- Attach relevant documentation
- Link related exception requests if applicable

Exception Request Attachments						Add New
Name	Size	Type	Upload Date	Downloads	History	
No Records Found						

Related Exception Requests			Add New	Lookup
Exception ID	Organization	Expiration Date		
No Records Found				



The sections at the bottom of the record provide the options to add Compensating Controls, Exception Requests Attachments, and Related Exception Requests.

Identify any controls that compensate for the exception. You can either select from a Control in the system, or provide a description of other controls that may be in place in the Additional Compensating Controls text box. Attach related documentation if necessary, and look up other exception requests related to this one.

When the Exception Request is ready for submission, change the Submission Status to *Submit for Review* and save the record. This will send a notification to the Reviewer you previously identified.

# Review and Approvals



- Reviewer will update Management Review section and update the Review Status

The screenshot shows a web application window titled "Exception Requests: EXC-23". The interface includes a menu bar with options like New, Copy, Save, Apply, View, Delete, Export, Print, and Email. Below the menu, there are two tabs: "Exception Declaration" and "Review and Approvals". The "Review and Approvals" tab is active, showing a form with several sections:

- About**: A collapsed section.
- Management Review**: A section containing several fields:
  - Review Status:** Awaiting Review
  - Review Date:** (Empty)
  - Risk Rating:** (Empty)
  - Risk Description:** (Empty)
  - Reviewer Comments and Conditions:** (Empty)
  - Reviewer Role:** (Empty)
  - Submitter Requested Date:** 2/25/2016
  - Approval Expiration Date:** (Empty)
- Review Attachments**: A table with columns for Name, Size, Type, Upload Date, Downloads, and History. It currently shows "No Records Found".



When the Exception Request has been submitted, the Reviewer will go into the system and review the record.

- The Reviewer will ultimately decide whether to accept or reject the exception in the Review Status field.
- Provide the **Reviewer Role** if desired and select the **Review Date**.
- The Requested Expiration Date will appear in the **Submitter Requested Date** field. The Reviewer can decide whether the requested date is reasonable, or if it needs to be moved, and record the final date in the **Approval Expiration Date** field.
- The Reviewer can also provide a **Risk Rating** to indicate how risky it will be to accept the risk in question, and provide justification for the selection in the **Risk Description** field.
- The **Reviewer Comments and Conditions** text box can be used to provide extra notes on the exception, or to list any caveats. For example, the Reviewer can indicate the Exception will be approved under the condition that the Submitter add another Compensating Control to this risk.

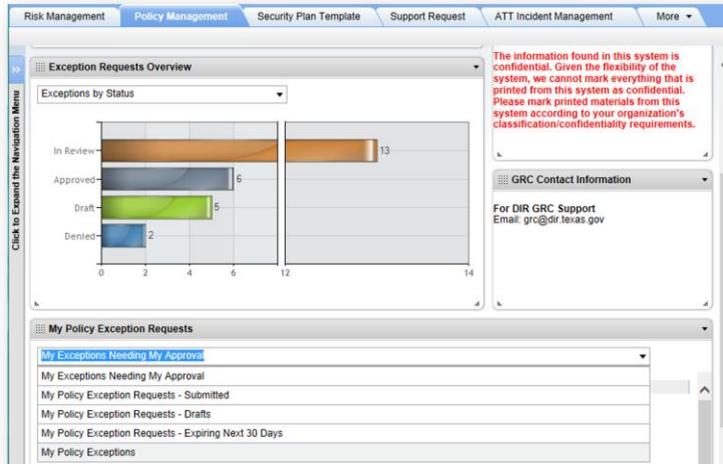
Finally, if there is documentation to attach, it can be attached to the Review Attachments section.

If the Reviewer decides to reject the Exception, the Submitter will need to go back into the record to make updates and resubmit it for approval. If the Reviewer approves the Exception, the Submitter's job is done.

# View Your Complete Exception



- Confirm your Exception appears in the Policy Exception Management dashboard



When you are finished with the Exception, confirm you can find it recorded in the system. It should appear on the Policy Exception Management dashboard. You can use either the Exception Requests Overview graph to find your exception if you know what Status it holds, or you can locate it using one of the dropdown menu options in the My Exception Requests iView.



# Security Plan Template Process



Now, let's dig into the applications that make up the Security Plan Template solution.

# Overview

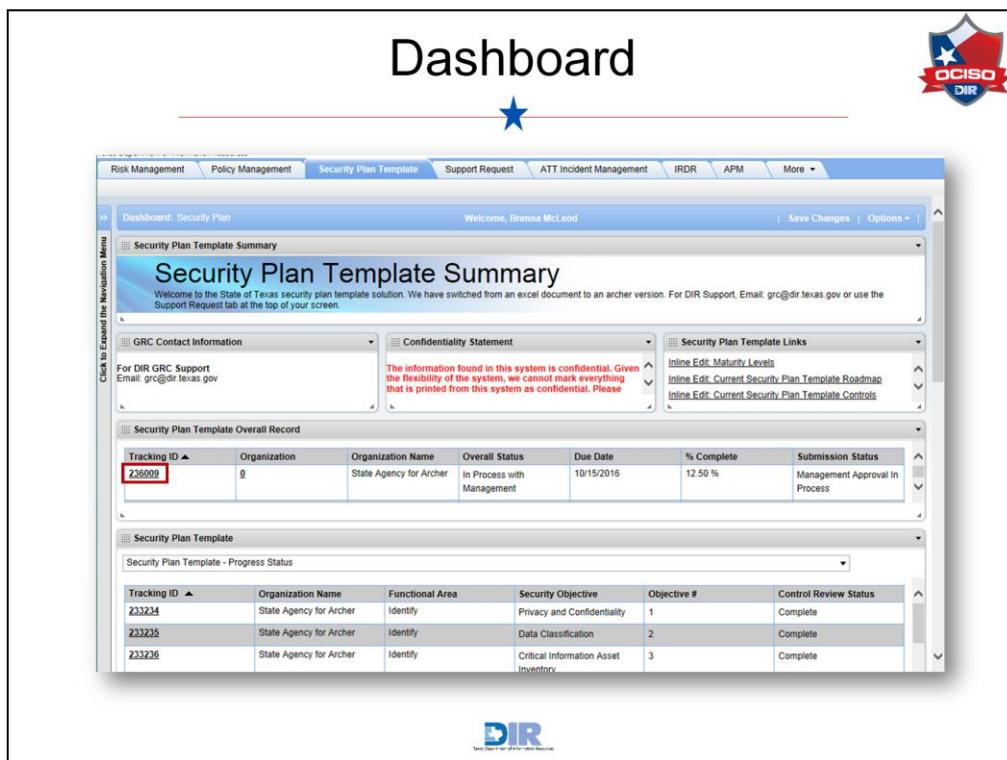


- Security Plan Templates need to be submitted by October 15 of even-numbered years
- If your Organization submitted the Security Plan Template using the excel sheet provided by DIR in 2014, your data has been recorded and archived in Archer
- If your organization submitted the Security Plan in a different format in 2014, you will not have archived data
- DIR hopes you can use this application to monitor your Key Controls regularly – not just for submission



Just a few quick notes before we dive into the solution:

- Security Plan Templates need to be submitted by October 15 of even-numbered years.
- If your Organization submitted the Security Plan Template using the excel sheet provided by DIR in 2014, your data has been recorded and archived in Archer.
- If your organization submitted the Security Plan in a different form in 2014, you will not have archived data.
- Finally, DIR hopes you can use this application to monitor your Controls on a regular basis – not just when it comes time to submit the Controls to DIR.



On the Security Plan Template dashboard, you will see similar iViews as in the Policy Exception Management dashboard: a solution Summary, Contact Information, a Confidentiality Statement, and Quick Links. The Quick Links featured in this dashboard all relate to Inline Editing, which is a quick way to make a lot of updates to your organization’s key controls. We’ll take a closer look at inline editing later in this training.

The next iView holds the Security Plan Template Overall Record. Each organization needs to submit 40 Key Controls, and instead of submitting each of those Controls individually, DIR has created one Security Plan Template Overall Record to house all 40 of those Key Controls. This way you are only submitting one Overall record once each Control has been updated. You will only see your organization’s Overall Record.

The Security Plan Template iView displays each of the 40 Key Controls so you can quickly access a specific Control from the Dashboard if necessary. This iView also serves to display how many of your Controls have been Reviewed, and how many still need to be completed. You will only see your organization’s Controls here, as well.

Let’s first look at the Security Plan Template Overall Record.

# Security Plan Template Overall Record



- Make updates to the General Information
- Either click into each Key Control, or use Inline Editing to make updates

Tracking ID	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	Organization Priority	Roadmap	Challenges to Implementation
233234	Privacy and Confidentiality	100	Complete	0	0	0	0	50	50	High	roadmap	Inadequate Funding Lack of Planning to Devise Roadmap No Changes Needed
233235	Data Classification	100	Complete	0	100	0	0	0	0			



Here, we have opened the Security Plan Template Overall Record and clicked the Edit icon to enter Edit mode. You'll first see a section on General Information. View identifying information on the record including the Tracking ID, Organization Number, and Organization Name here. You can update the Record Version, Submitter name, Submission Status, and Submission Date.

The Security Plan Controls section is where you can find the 40 Controls that must be submitted. If you have archived data from 2014, you will need to document the differences between the previous submission, and where your Controls stand now. If not, you will follow the same process, but you will not have the data from 2014 in the system.

The next step will be to make updates to the Controls. To do that, you can either go into each Control individually, or use the inline editing feature. We'll look at both, but let's start with clicking into a Control record.

# Security Plan Control Record



- Add specific activities in place to carry out the Control
- Update the Control Review Status once the Security Office completes the review for your reference

General Information	
Tracking ID:	233234
Organization:	0
Objective #:	1
Security Objective:	Privacy and Confidentiality
% = 100:	<input checked="" type="checkbox"/>
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.
Record Version:	Current
Organization Name:	State Agency for Archer
Functional Area:	Identify
Reporting Year:	2016
Control Review Status:	<input type="radio"/> Not Complete <input checked="" type="radio"/> Complete <a href="#">Edit</a>

▼ Relevant Controls

Relevant Control Activities in Place: relevant activities



In edit mode on the first listed Key Control, note the only field you can edit in the General Information section is whether the Control Review has been completed by the Security Office. This field exists for internal use in your organization – you can use this field to flag the Control as Incomplete, or mark it as Complete when you finish updating it.

In the Relevant Controls section, you can add the specific activities in place within your organization to carry out the Control.

# Associated Controls



- Associated Controls are the Control Procedures linked to this Key Control
- Click *View All* to see all Associated Controls

Procedure Name	Procedure ID	Organization	Functional Areas	Functional Sub-Areas	Total All Findings	Total Open Findings	State Implementation Date
Publicly Accessible Content	AC_22.0	0	Identify	Privacy and Confidentiality	0	0	2/1/2017
System Interconnections	CA_03.0	0	Identify	External Vendors and Third Party Providers Privacy and Confidentiality Security Assessment and Authorization / Technology Risk Assessments	0	0	2/1/2016
Transmission Confidentiality and Integrity	SC_08.0	0	Identify Protect	Privacy and Confidentiality System Communications Protection	0	0	2/1/2015
Software, Firmware, and Information Integrity	SI_07.0	0	Identify	Privacy and Confidentiality	2	1	
Authority to Collect	AP_01.0	0	Identify	Privacy and Confidentiality	0	0	



Under the Relevant Controls section is a section for Associated Controls. These are Control Procedures related to this Key Control. You can see how many assessment findings you have which may help you determine the maturity level of the key control. Be sure to click *View All* to see the full list of Associated Controls.

# Maturity Levels



The screenshot shows a software interface for a Security Plan Template (ID: 233234). It displays five maturity levels: Level 0 (Non Existent), Level 1 (Initial), Level 2 (Repeatable), Level 3 (Defined), and Level 5 (Optimized). Level 4 (Managed) is currently selected. The interface includes a table for Level 4 with the following details:

Level 4 Pattern Controls:	Description
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. <input type="text" value="50"/> %
How is Effectiveness of the Control Measured?:	effective

A 'General Information' pop-up window is overlaid on the bottom right, containing the following data:

General Information	
Tracking ID:	233234
Organization:	0
Objective #:	1
Security Objective:	Privacy and Confidentiality
% = 100:	<input type="checkbox"/> X

The next step in the Key Control is to update the Key Control Maturity Levels. You'll read the descriptions at each level, and determine where your organization falls within those categories. In this example, 50% of Organization 0 falls under Level 4 maturity, where its "structure supports a focus on privacy and confidentiality," and it "uses an established risk management framework to measure and evaluate risk and integrate improvements beyond the requirements of applicable regulations." For Levels 4 and 5, you are asked to provide comments on how the effectiveness of the Control is measured.

Your total percentage across all levels needs to add up to 100%. If not, you will see a red X in the % = 100 field in the General Information section.

# Challenges and the Roadmap



- Identify Challenges to Implementation
- The Roadmap section is optional, but can be tracked on the Dashboard if used

The screenshot displays a web-based interface for a Security Plan Template (ID: 233234). It features two main sections: 'Challenges to Implementation' and 'Roadmap'. The 'Challenges to Implementation' section includes a list of checkboxes for 'Inadequate Funding', 'Inadequate Staffing', 'Lack of Planning to Develop Roadmap', 'No Changes Needed', and 'Organizational Support'. The 'Roadmap' section includes a dropdown for 'Organizational Priority' (set to 'High'), 'Start Date' (3/2/2016), 'End Date', and a text area for the roadmap description. It also has radio buttons for 'Roadmap Status' (Not Started, In Progress, Completed, Not Applicable) and an 'Add' button for 'Roadmap Attachments'.



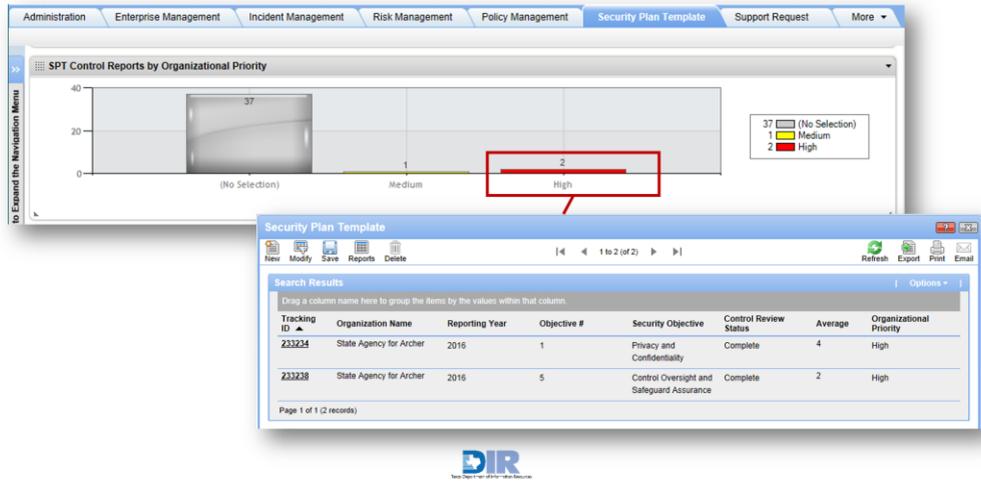
After the Levels of Maturity are complete, move into the section on the Challenges to Implementation and the Roadmap. Identify any challenges to implementation your organization faces, and attach any documentation surrounding those challenges if desired.

Your Organization should use the Roadmap section to plan out how to improve the implementation of a Control. You can mark the Organizational Priority of the Roadmap, select target Dates, and provide a plan in the Roadmap text box. The Status can also be tracked, and you can add attachments. We'll take a moment here to show you where the Roadmap information can be tracked on the Dashboard.

# View Roadmap Report



- Organizational Priority refers to the Priority assigned to the Roadmap
- Quickly view the full list of High Priority Controls



On the Security Plan Template dashboard, you'll see an iView on Security Plan Template Control Reports by Organizational Priority. The Organizational Priority in the title refers to the Priority assigned to the Roadmap. In this example, 37 Key Controls do not currently have a priority assigned to the Roadmap, 1 Key Control has a Medium Priority, and 2 have a High Priority. You can click on the bar graph to quickly view your Key Controls with an important Roadmap priority.

Now let's return to our Key Control record.

# Scores/Results and Archived Records



- Average is your organization's Average maturity level for this Controls
- View previous submission's maturity levels

The screenshot shows a software interface for 'Security Plan Template: 233234'. It features a menu bar with options like New, Copy, Save, Apply, View, Delete, Export, Print, and Email. The 'Scores/Results' section includes a summary table:

Total Percentage:	100 %	Average:	4
Total Open Findings:	1	Total All Findings:	2

Below this is the 'Archived Security Plan Template' section with a table of records. The first record is highlighted with a red box around the '% of Agency at Lvl 0' column.

Tracking ID	Organization	Organization Name	Reporting Year	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
238752	0	State Agency for Archer	2014	Privacy and Confidentiality	100 %	0 %	0 %	0 %	0 %	0 %



The Scores and Results section displays the percentage complete, and the Average Maturity Level. In this example, Levels 4 and 5 were both at 50%, so Archer displays the lower maturity level as the average. As another example, if you have 20% Level 2 maturity, 50% Level 3 maturity, and 30% Level 4 maturity, your Average level will display as Level 3.

You can also find the Total Open Findings, and Total Findings, whether Open or Closed.

The Archived Security Plan Template section displays previously submitted Security Plans. Here, we can see that in 2014 Organization 0 had no privacy policy at all.

# View Your Updated Key Control



- Confirm your changes have been recorded in the Security Plan Template Overall Record

Security Plan Template Overall Record: 236009

General Information

Tracking ID:	236009	Record Version:	Current
Organization:	0	Overall Status:	In Process with Management
Due Date:	10/15/2016	Organization Name:	State Agency for Archer
Submitter:	Sally_Smith	Reporting Year:	2016
Submission Status:	Management Approval In Process	Submit Date:	11/17/2015
% Complete:	12.50 %	History Log:	<a href="#">View History Log</a>

Security Plan Controls

Tracking ID	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	Organizations Priority	Roadmap	Challenges to Implementati
233224	Privacy and Confidentiality	✓	Complete	0	0	0	0	50	50	High	This organization needs to immediately complete the following steps...	Inadequate Funding Lack of Planning to Develop Roadmap No Changes



When you are finished updating your Key Control, save your changes and return to the Security Plan Template Overall Record to confirm your updates have been recorded. You can then move on to the next Key Control.

Let's take a look at another approach to updating the Key Controls.

# Inline Editing



Security Plan Template Overall Record: 236009

Tracking ID	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	Challenges to Implementation
23324	Privacy and Confidentiality	Open	Complete	0	0	0	0	0	0	High		Inadequate Funding
23325	Data Classification	Complete	Complete	0	100	0	0	0	0	No Selection		
23326	Critical Information Asset Inventory	Open	Complete	0	0	50	50	0	0	Low		
23327	Enterprise Security Policy, Standards and Guidelines	Open		0	0	0	0	0	0	Medium		
23328	Control Oversight and Safeguard Assurance	Open		0	0	0	0	0	0	High		

Rich Text Editor

This organization needs to immediately complete the following steps...

OK Cancel

- Click *Enable Inline Edit*
- Edit any column with the pencil icon
- Click into a field to update it

You can edit your Organization's Maturity Levels using the Inline Editing feature to expedite the process. You can either click the Enable Inline Edit link, or enter the Edit mode to reveal the inline editing. You can edit any column with a pencil icon next to it. Click directly into the field you want to update. You can type in a new percentage, select a different Organizational Priority, and even edit the Roadmap or Challenges.

# Saving Inline Edit Changes



- Each Save icon only saves one record
- Click the Save Changes button to save all updates

Security Plan Template Overall Record: 236009

This record has pending related record changes: **Save Changes**

Security Plan Controls | Disable inline edit | View All

Tracking ID	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	Challenges to Implementation	
233234	Privacy and Confidentiality	✓	Complete	0	0	0	0	50	50	Medium	This organization needs to immediately complete the following steps...	Inadequate Funding Lack of Planning to Develop Roadmap No Changes Needed	
233235	Data Classification	✓	Complete	0	90	0	10	0	0				
233236	Critical Information Asset Inventory	✓	Complete	0	0	50	40	10	0				
233237	Enterprise Security Policy, Standards and	✓	Complete	0	90	10	0	0	0	Medium		Inadequate Staffing No Changes	



As you make changes to each record, a save icon will appear on the right side of the screen. Please note that each icon only saves changes to the record in which it appears. To save all of your changes, click the Save Changes button at the top of the screen.

# Management Approval



- Identify who needs to approve the overall record
- Update the Submission Status

The screenshot displays a web application interface for a Security Plan Template Overall Record (Tracking ID: 236009). The interface is divided into two main sections: Management Approval and General Information.

**Management Approval Section:**

- Approval By:** A text input field.
- Approval Date:** A date input field.
- Approval Comments:** A large text area for entering comments.
- Approval Attachments:** A text input field with an "Add" button.
- Approver Role in Organization:** A list of radio button options: CIO/IRM, CISO/ISO, Organization Head, and Other. The "Other" option is selected, and a text input field is provided for the role name. An "Edit" button is located below the options.

**General Information Section:**

- Tracking ID:** 236009
- Organization:** 0
- Due Date:** 10/15/2016
- Submitter:** Sally, Smith
- Submission Status:** A dropdown menu currently set to "Management Approval In Process". This section is highlighted with a red border.

When all of your Key Controls have been updated, you can identify who needs to complete the Management Approval section. Then change the Submission Status in the General Information section to *Management Approval In Process*. The Approver in your Organization will complete a review of the Security Plan Template Overall Record, make Comments, and provide any necessary attachments.

# Submitting the Record to DIR



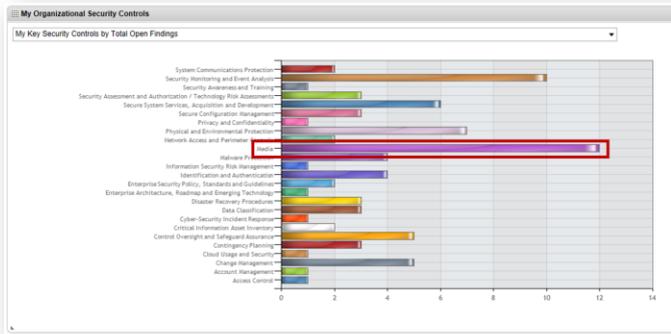
- Change the Submission Status to *Submitted to DIR*
- DIR will receive a notification that your organization's Security Plan Template is ready for review

General Information	
Tracking ID:	236009
Organization:	Q
Due Date:	10/15/2016
Submitter:	Sally, Smith ...
Submission Status:	Submitted to DIR  Edit



When the Management Approval section has been completed, the Approver will change the Submission Status to Submitted to DIR and save the record. DIR will receive a notification that your organization's Security Plan Template is ready for review.

## Dashboard, cont.



- View Controls by a specific filter
- Click on a bar to open the full list of records



Let's go back to the Security Plan Template Dashboard. The last piece of the dashboard displays Controls by a specific filter. Here, it is by Total Open Findings, but you can also see the Controls sorted by Functional Area or view your Organization's Controls tied to the Key Controls.

These reports are also interactive in that you can click one of the bars on the bar graph to be taken directly to the categorized set of records. For example, you can click the Media Security Control bar to see the 12 open findings in that category.



# Quiz



The next stage of this training is a brief quiz to check your learning. Click Next to continue.

By default, the only policies available in the policy portion of Archer are those pertaining to TAL 202. However, you have the option to add your own policies.

0: true  
0: false

## Archer Policy Quiz

Quiz - 10 questions

Last Modified: Mar 16, 2016 at 09:55 PM

### PROPERTIES

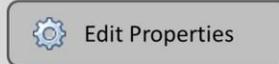
On passing, 'Finish' button: [Goes to Next Slide](#)

On failing, 'Finish' button: [Goes to Next Slide](#)

Allow user to leave quiz: [After user has completed quiz](#)

User may view slides after quiz: [At any time](#)

Show in menu as: [Multiple items](#)





# Searching and Reporting



Now that you know how to work with policy-related records in Archer, let's talk about how you can go back and find records at a later time.

# Overview



- Quick Search Concepts
- Advanced Search Concepts
- Statistics Search Concepts
- Creating Reports



Searching gives you the ability to locate specific records within content applications and to display values from multiple records on your screen. After running a search, you can save the search criteria as a named report, enabling you to easily access your search results at any time.

The application provides two primary methods of searching:

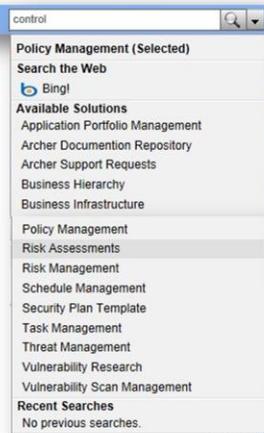
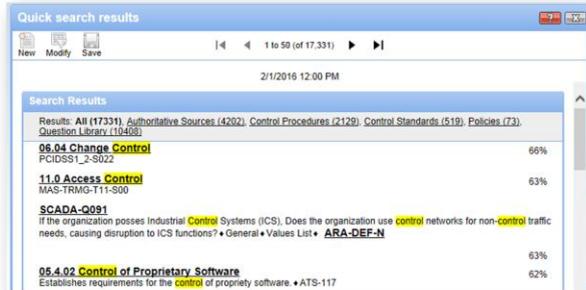
- Quick Search (from the top frame)
- Advanced Search (from the Navigation Menu)
- Statistics Searching allows you to create charts and graphs
- Creating Reports is simply a process to save the searches you have created

# Quick Search



Preferences Reports Help Logout

- Search across multiple applications within a solution
- Search the internet via Bing
- Recently searched keywords are remembered



The Quick Search feature in the top frame of the interface allows you to perform a keyword search in multiple Applications within a single Solution. The first selection in the dropdown will default to the first Solution in the current Workspace, but you may select another Solution to search, or even search the Internet using Bing. A list of your recently used keywords will appear at the bottom of the dropdown menu.

In this example, we have searched for the word “Control” in the Risk Assessments solution. The listing at the top of the search results shows us that 48 records were found that contain that keyword: 8 Application Assessment records, 10 Applications records, 13 Information Types records, and so on. Clicking any of the application names would lead us to a subset of the overall search results. Clicking a hyperlink in the search results shown below will take us to the linked record.

# Keyword Search Operators



Query Types	Example
Single keyword term	Document
Phrase	"important document"
Boolean Operators	Important AND (OR/NOT) document
Wildcard (single character)	Doc?ment
Wildcard (multi-character)	document*
Fuzzy search	document~
Grouping	(important OR urgent) AND document
Proximity Search	"important document"~5



You can use a widely accepted set of search operators to produce complex keyword searches. You may be familiar with some of these.

- Running a search using a **Single Keyword Term** searches the system for all records containing that word. In this case, it will return a listing of all records with the word *document* in it.
- When searching a **Phrase**, such as "important document," it is essential to enclose your phrase in quotation marks. If you do not use quotation marks, your search will return all records that contain the term "important" OR the term "document."
- **Boolean Operators** allow you to include or exclude terms using capitalized operators of AND, OR, and NOT. You must capitalize each operator in order to run your search effectively.
  - Using AND returns records including both terms "Important" and "Document"
  - Using OR returns records including either "Important" or "Document"
  - Using NOT returns records including the term "Important" but not the term "Document"
- The **Wildcard** operator can either be for a single character or a whole term.
  - The most common way to run a single character wildcard search is to place a question mark in place of any letter in the word. Running this wildcard search will return any records that might have a typo in the term. In this example, we have replaced the "u" in document with a question mark (doc?ment). The search will return records such as docum~~e~~nt, dockment, and docum~~e~~nt. All letters in the term will be matched, but the question mark tells the system to look for any character in that spot.
  - Searching an entire term as a wildcard search looks a little different. Use an asterisk after a string of characters to include terms that match your specified characters, and any characters the system finds attached to them. For example, a search on document\* will return documents, documenting, and documented.
- A **Fuzzy Search** returns all records that contain the term "document" and any other term that is similar in spelling. Fuzzy searching enables you to search for keywords that may be misspelled within records, so if you

search for “document~”, your search will also return records that contain “dokument,” “documant,” etc. Please note that the tilde symbol (~) must appear directly after the term with no space between the term and the symbol.

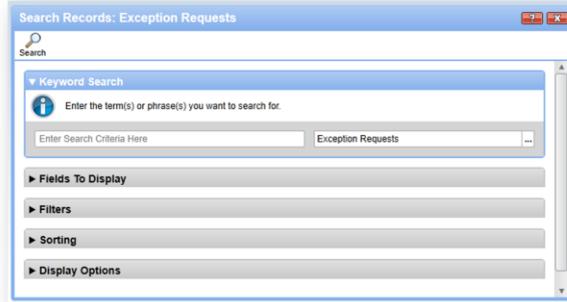
- A **Grouping** search combines Boolean operators to search for a specific string of terms. In this example, we have (important OR urgent) AND document. This search will return records including “important document” and “urgent document.”
- The **Proximity** search returns records in which the keywords are within the specified number of words from each other. In the example given, records will be returned only where “important” OR “urgent” is within 5 words of the word “document”.

# Advanced Search Overview



- Accessible via the Navigation Menu for each application

- Options:
  - Keyword Search
  - Fields to Display
  - Filters
  - Sorting
  - Display Options



From the Navigation Menu, you can execute an advanced Search by clicking the Search Records link under any content application.

Clicking this link opens the Search page for that application, which enables you to keyword search for specific records, to format the display of your search results and to define filter criteria to narrow the results of your searches.

# Keyword Search



- Enter keyword(s) and/or phrases
- Search the targeted application
- Can include other applications in the search once relationship has been established

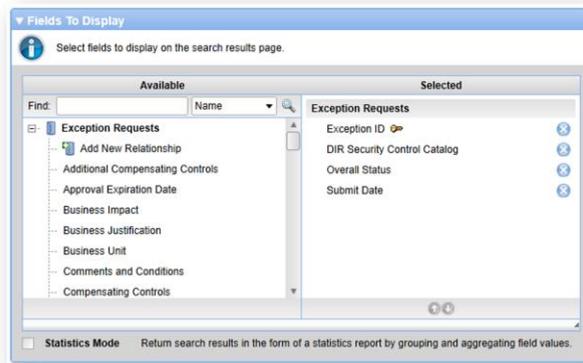
A screenshot of a web application's 'Keyword Search' interface. The window has a blue title bar with a dropdown arrow and the text 'Keyword Search'. Below the title bar is a grey information icon and the text 'Enter the term(s) or phrase(s) you want to search for.'. There are two search input fields. The first field contains the text 'In Review AND AC-01|'. The second field contains the text 'Exception Requests' and has an ellipsis button to its right.

The Keyword Search option allows for the same search operators as the Quick Search. Unlike the Quick Search, which searches all Applications in a single Module, the Keyword Search on the Advanced Search page searches within a single Application. This allows for a more targeted search. If you create a relationship between two applications, you can use the ellipsis button to request that the keyword be searched in both applications. We'll explore that on the next slide.

# Fields to Display



- Select the fields to be returned with the search results
- Rearrange field order
- Include fields from other application
- Can opt to enforce relationships



In the Fields to Display section, you can select the fields of data that should display in your search results. Once you have selected your fields to display, you can also arrange those fields so they display in the desired order.

If the application you are searching in is related to another, you can click Add New Relationship to create a searching relationship between the Applications. You can then select fields from the related application to display in your search results.

Once you have created relationships for searching purposes, you can click the Configure Relationships link to require the system to only return records from the first application that also have a related record within the second application. For example, you might show all Control Procedures that have one or more Exceptions associated to them.

# Filters



- Allows users to view a subset of the overall data set
- Evaluate the data in most field types
- Operators:
  - Equals / Does Not Equal
  - Contains / Does Not Contain
  - Greater Than / Less Than
  - Between
  - Last / Next
  - After Today / Prior to Today
  - Current

Field To Evaluate	Operator	Value(s)	Relationship	Actions
1. DIR Security Control Catalog	Contains	AC-01 AC-03 AC-02	And	
2. Overall Status	Equals	Approved	And	

Advanced Operator Logic:  Example (1 AND 2) OR 3



The Filters section allows you to specify a subset of information to be found. For example, if you wanted to look for all Exception Requests with an Overall Status of Approved, you would filter on the *Overall Status* field to Equal “Approved.” You can combine multiple filters, and can also specify the logic to be used related to the filters, such as “(filter 1 AND filter 2) OR filter 3.”

# Current User Filter



- Available for fields that reference user accounts
- Allows the creation of a single report to display user-specific data rather than individual reports for every user
- The report will always be filtered to display appropriate information based on the user executing the report

The screenshot shows a 'Filters' window with a table of filter rules. The first rule is for the 'Submitter' field, using the 'Equals' operator and the value 'Current User'. The relationship is 'And'. There is also an 'Advanced Operator Logic' section with an example '(1 AND 2) OR 3'.

Field To Evaluate	Operator	Value(s)	Relationship	Actions
1. Submitter	Equals	Current User	And	⊗
2.			And	⊗

Advanced Operator Logic:  Example (1 AND 2) OR 3



If you want to create a report in an application with a field that references user accounts, you can filter your search results so they display only records relevant to the user who is viewing them.

The "Current User" filter allows you to create a report that dynamically adjusts content based on the user executing the report. For example, you could create a "My Plans" report for your Plan Managers team.

- When Plan Manager A executes the report, only the plans assigned to him would be displayed.
- When Plan Manager B executes the report, only the plans assigned to her would be displayed.

Using this feature, you can create a report that will display information dynamically, dependent upon the current user.

# Sorting



- Sort on multiple fields by ascending or descending order
- Enable grouping if desired



▼ Sorting | Add New |

Select fields from the list below to sort your data. You can choose to sort ascending or descending and also to group data if desired.

Field	Order	Grouping	Actions
1. DIR Security Control Catalog ...	Ascending ▼	Enabled ▼	
2. Expiration Date ...	Ascending ▼	Disabled ▼	



The Sorting section allows you to define how you want the search results to be sorted. If you do not specify any sorting here, the records will be sorted based on their key fields. You can always click on column headers in the actual search results to sort the results later as well.

# Display Options



- Display format options:
  - Column – Hierarchical
  - Column – Flat
  - Row
  - Summary
  - Card
  - Calendar
- Can limit the number of records returned
- Can fix headers so that the column names remain visible as user scrolls

A screenshot of the 'Display Options' dialog box. The dialog has a title bar with an information icon and the text 'Display Options'. Below the title bar is a subtitle: 'Configure display options, including sort order, results format, heading options and results per page.' The main area contains several controls: 'Display Format:' with a dropdown menu set to 'Column - Hierarchical'; 'Results Per Page:' with a dropdown menu set to '50'; 'Record Count:' with a dropdown menu set to 'All Records'; 'Headings:' with two checkboxes: 'Criteria' (unchecked) and 'Date' (checked); and a section for 'Expand All Results', 'Fix Headers' (checked), and 'Enable Inline Edit' (unchecked). Each checkbox has a corresponding description.

Six display options are available for standard searches:

- Column - Hierarchical
- Column - Flat
- Row
- Summary
- Card
- Calendar

In addition, you may adjust the number of results returned per page and/or opt to only display a finite total of records (i.e. display only 10 of the possible 5,000 records.)

Just as you can freeze the top row of cells in Excel to serve as column headers, you can perform a similar function in Archer by fixing the headers in a search.

# Display Results – Column Options



- Both options display results in rows and columns
- Useful if results will be exported
- Hierarchical format:
  - Allows users to group results by one or more fields
- Flat format:
  - Displays results in a simple, non-grouped format

Search Results

Exception ID	DIR Security Control Catalog	Overall Status	Submit Date
DIR Security Control Catalog:			
DIR Security Control Catalog: AC-01			
EXC-1	AC-01	In Review	11/20/2015
EXC-10	AC-01	In Review	11/20/2015
EXC-22	AC-01	Approved	1/19/2016
DIR Security Control Catalog: AC-02			
EXC-4	AC-02	Denied	11/17/2015

Page 1 of 1 (22 records)

Search Results

Drag a column name here to group the items by the values within that column.

Exception ID	DIR Security Control Catalog	Overall Status	Submit Date
EXC-2		Approved	11/16/2015
EXC-3		Approved	11/16/2015
EXC-5		Draft	

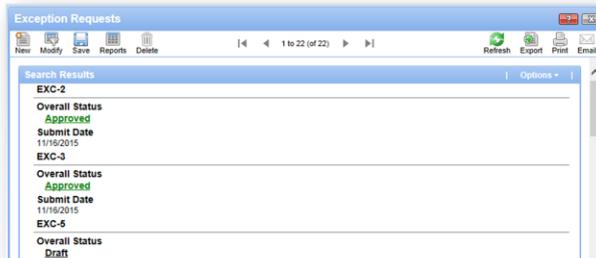


The column display options are hierarchical and flat. Hierarchical results will allow you to group your results by a common field. Flat results look similar to a simple spreadsheet with all selected fields displayed in a grid.

# Display Results – Row



- Displays results in rows
- Each record's fields are stacked vertically
- Records are separated by horizontal lines
- Empty fields will not be displayed
- Useful if results will be printed



The Row format allows you to create a clean report with each record's fields separated from the one below by a horizontal line.

# Display Results – Summary



- Displays results in a block format
- All field names are omitted
- Key field serves as a heading for each record

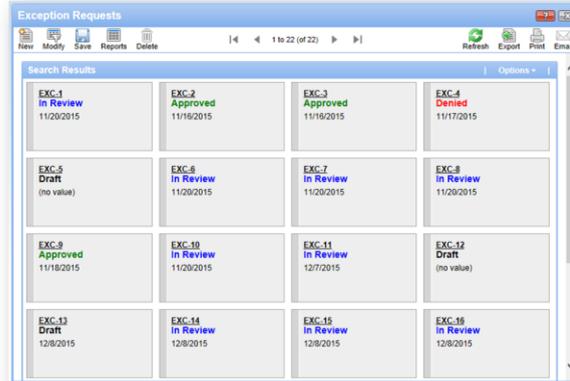


The Summary option allows you to display results in a block format. The values in each selected field are shown, but the actual field names are excluded in this view.

# Display Results – Card



- Displays results in a series of rectangular boxes
- Similar to the Contacts view in Outlook
- Only includes fields from the primary application or first level searched

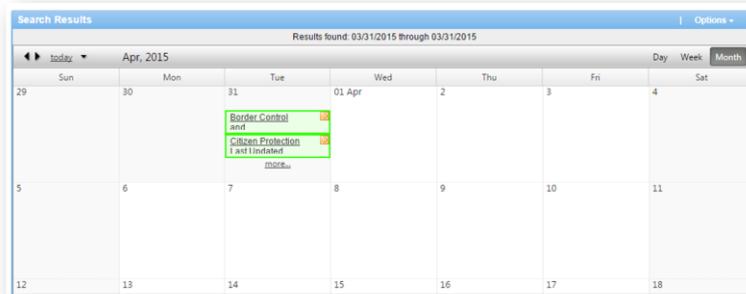


The Card display option allows you to mimic the Microsoft Outlook Contacts view. Only a small number of fields will be shown in this view, regardless of how many fields are selected for display.

# Display Results – Calendar



- Displays results plotted on a calendar
- Can designate colors for different fields (i.e. green for Start Date, red for End Date)
- Can toggle between day, week and month views
- Can create events in one-hour blocks or all-day events
- Each date includes an iCalendar option



The Calendar display option allows you to plot dates in a calendar format, and you can specify different colors for different fields (for example, a “Reported Date” field might be displayed in red, and a “Resolved Date” field in green.) The Calendar option allows you to display results in day, week, and month views. Each calendar item includes an iCalendar icon to allow users to easily add important dates to their own Outlook calendars.

## Search Results Toolbar



---



New Modify Save Reports

|< < 1 to 29 (of 29) > >|

Refresh Export Print Email

- New: allows user to add a new record to the primary application
- Modify: Allows user to redefine current search
- Save: Allows user to save search as a report
- Reports: Allows user to select from a saved list of reports



Any time you run a search, you will see a new toolbar at the top of the search results.

- New – allows you to add a new record to the primary application from your results.
- Modify – allows you to redefine your search criteria and run the search again.
- Save – allows you to save your search criteria as a report that can be executed as often as you wish.
- Reports – allows to quickly execute reports previously saved from the primary application of your search.

## Search Results Toolbar, cont.



- Refresh: Re-runs the search
- Export: Allows user to export the search results to:
  - Rich Text
  - PDF
  - Excel
  - CSV
  - HTML
  - XML
- Print: Allows user to print the search results
- Email: Allows user to send a link to the saved search results

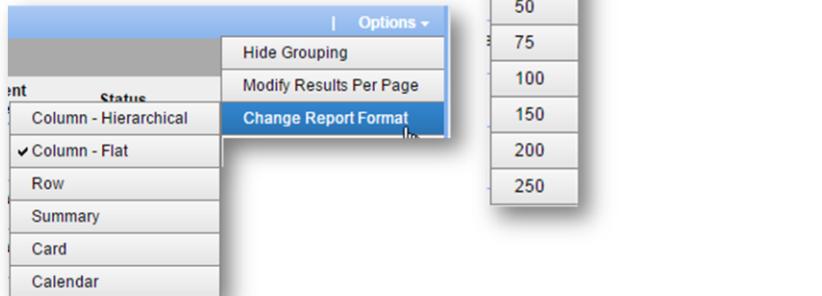


- Refresh – re-runs the same search again to display the records that now match the search criteria.
- Export – allows you to export the records from your search into a variety of available formats.
- Print – allows you to print your search results.
- Email – this icon becomes active only after you have saved search results as a report. Clicking this icon will open a new email message that includes a link to the saved report. Just as with the linked emails you can send from an individual record, the recipient of the email must have appropriate access rights established to access the link. The actual report itself is not sent with this icon.

# Search Options



- Hide Grouping
- Modify Results Per Page
- Change Report Format



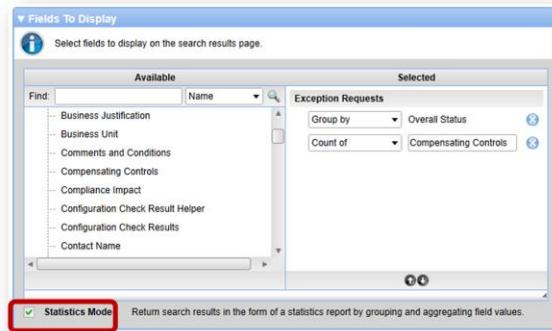
Within each Search Results page, there is an Options dropdown menu in the upper right corner. Depending on the type of search run, you may see the following options:

- Hide Grouping – Selecting to hide the grouping option will remove the gray “grouping” area that appears just below the same bar that includes the Options dropdown menu.
- Modify Results Per Page – This option allows you to extend (or reduce) the number of results returned per page. Options include 10 through 250 results per page.
- Change Report Format – This option allows you to change the search results format displayed without having to return to the Display Options section of the Advanced Search page.

# Statistics Search Overview



- Can perform single or multiple series charting
- Where: Advanced Search > Fields to Display section
- How: Check the Statistics Mode box
- Add fields and select the functions:
  - Group by / Group by
  - Count Of
  - Average Of
  - Median
  - Mode
  - Sum Of
  - Minimum
  - Maximum



The Search page also provides controls for creating statistical reports by grouping and aggregating field values. To run a statistics search, complete the following steps:

1. Select the Statistics Mode checkbox, which is located under the Available list in the Fields to Display section. Selecting this option will clear any selected display fields, enabling you to create your statistical report from scratch.
2. Add the field(s) on which you want to apply grouping or aggregate functions.
3. Select the grouping or aggregate function you want to apply. Grouping and aggregate functions include the following options:
  - Group by / Group by (day, week, month, quarter)
  - Count Of
  - Average Of (numeric and voting fields only)
  - Median (numeric and voting fields only) – This is the centermost value
  - Mode (numeric and voting fields only) – This is the value that occurs most often
  - Sum Of (numeric and voting fields only)
  - Minimum (date, numeric and voting fields only)
  - Maximum (date, numeric and voting fields only)
4. Run your search.

# Display Search as a Chart



- Initial results are returned as Data Only format
- To convert results into a chart, select a charting option from the charting toolbar



- Several chart types available
- Multiple customization options available for each chart type:
  - 2D or 3D options
  - Colors are fully customizable
  - Various shading options are available
  - Transparency can be adjusted
  - Legend and labels can be repositioned



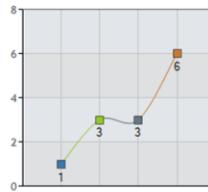
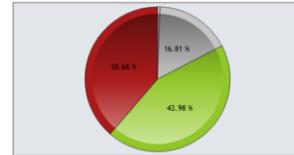
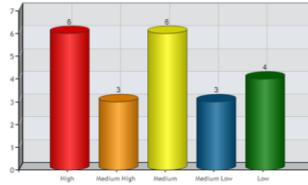
When you execute a statistics search, the results of your search will initially display as statistical data in a table. Assuming your search results are chartable, a new Charting toolbar will appear at the top of the search results. This toolbar allows you to display this data in chart form, which provides you with a more concise, visual presentation of the information. We will discuss each of these toolbar options in a moment.

To enable the charting feature, the “Group by” function must be the first function listed in the Selected pane within the Fields to Display section on the Advanced Search page. If an aggregate function is listed first, the Charting toolbar will not display.

# Chart Types



- Vertical bar (default)
- Horizontal bar
- Pie
- Donut
- Gauge
- Funnel
- Line
- Bubble
- Radar
- Heat Map



- 1 February 2012
- 3 March 2012
- 3 April 2012
- 6 June 2012



Based on the search performed, various chart types may be available for you to further customize your report. Each chart type carries its own customization options that we'll explore as we look at the charting toolbar.

# Charting Toolbar



- 3D: Allows you to toggle between 2D and 3D rendering
- Chart Options: Lists the display variations available for the selected chart type
- Chart Colors: Enables user to specify the color properties for the data series, the legend and the plot area



- The 3D checkbox allows you to toggle between 2D and 3D rendering of a chart.
- The Chart Options dropdown menu lists the display variations available for the selected chart type. Any time you change the chart type, the Chart Options dropdown menu is dynamically updated to display the correct options for the selected chart type.
- Clicking the Chart Colors icon opens the Chart Colors dialog, which enables you to specify the color properties for the data series, the legend and the plot area.

# Charting Toolbar



- Transparency Level: Enables user to control the transparency level of the plotted area
- FX: Lists the shading, smart break and threshold effects that you can apply to the data series
- 321: Allows the user to control the position of the legend, the display of value labels and labeling of the X and Y axes



- The Transparency Level dropdown menu enables you to display the chart's data series as opaque (solid) or transparent to some degree. Available transparency levels include 25%, 50% and 75%. By default, data series are displayed as Opaque.
- The Shading Effects dropdown menu lists the shading (light casting) effects that you can apply to the data series based on the currently selected chart type and whether the chart is set to display in a 2D or 3D format.
- The 321 dropdown menu provides the options for positioning the legend relative to the plot area of the chart. By default, the legend position is set to Top Right. This also controls the Value Labels with options for displaying numeric value labels relative to series data points (e.g., bars or pie slices) within a chart. The available options vary depending on the selected chart type.

# Reporting Basics



- Any search can be saved as a report
- Reports can be personal or global
- All reports are real-time snapshots of the data at the time of execution
- Reports can be modified and saved as a new report
- The results of any report can be exported



Let's go back and talk about the Save and Reports icon on the Search Results toolbar. Once you have created a search that you want to save to run again at another time, click the Save icon in the toolbar. Depending on your level of access for the Application you're searching, you may be able to save the report as a global report, which you can then share with others. All reports are simply a saved set of search criteria, so each time you access a report, you're actually re-running the search. This ensures you always have real-time data in your report. Once a report has been saved, it can later be modified and either saved as an entirely new report, or the changes can be saved to the original report. Reports can be displayed in iViews on a dashboard, can be exported into a variety of formats, and can be accessed from either the Reports icon dropdown arrow or the Master Reports Listing at the top of the Archer interface.

# Personal Vs. Global Reports



- Personal Reports
  - Available only to the person who saved the report
  - Can be promoted to a global report
- Global reports
  - Can be shared with multiple people
  - Can only be created by users with global report creation access



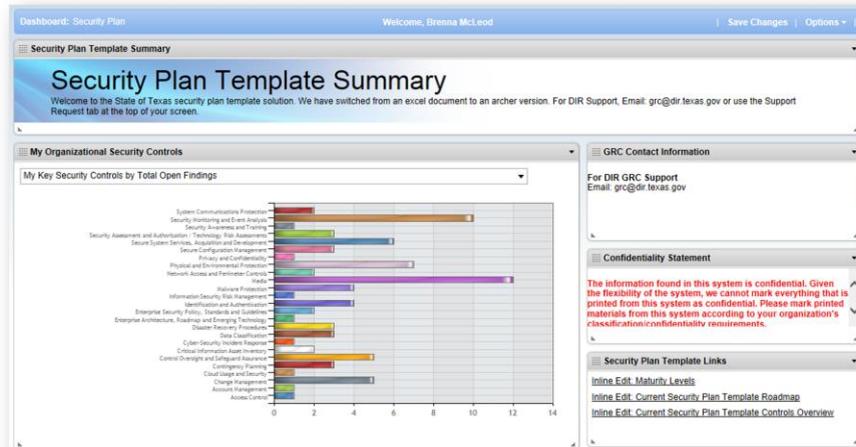
A Personal report is a private report. Only the user who created it can access it. You can send a link to your Personal report to another user, but when that user opens the link, the report will be re-run using the criteria from your search. Note that if you are trying to send a set of records to another user, you should use the export icon. Exporting your results ensures the information you want to send will be sent without re-running the search.

A Global report is a report that can be shared with other users. Other users will be able to see a Global report in the Master Reports Listing and other areas where reports are shown (Dashboard, Navigation Menu, Reports icon.) Global reports may be permissioned to all other users, a select group of users, or even just one other person. Only users with some kind of administrative access will have the option to save Global reports.

# Display Reports



- Reports can be displayed within iViews for end users to see upon accessing a Dashboard.



Once saved, reports can be also displayed within iViews for end users to see upon accessing a Dashboard, bringing us full circle.



Thank you.



This concludes Policy Management End User Training in the Archer system. As always, we thank you for your time.