Galvanize

Welcome to Rsam
Basic Administrator Training

Introduction and Logistics

Agenda

Day 1

- Rsam Community
- Rsam Support
- Rsam Building Blocks
- Introduction to Rsam / Best Practices
- Structures & Elements (Overview)
- Structures & Elements (Records)
- Administrator Groupings & System Roles

Day 2

- User Permissions & Roles
- Workflow
- Risk Analytics
- Data Import
- Searches & Charting
- Home Screens & Home Page Designer

Day 3

- Reporting
- Structures & Elements (Objects)
- Email Notification
- Email Listener
- Rsam Scheduler
- Rsam Basic Admin Exam (optional)

Rsam Support Options

Rsam Support Offering & Contact Numbers

- Currently offers 3 levels of support
  - Bronze (8am – 8PM EST Monday thru Friday)
  - Silver (24 / 5 Monday thru Friday)
  - Gold (24 / 7)
- By Phone
  - 201-875-3456 and 1-800-726-Rsam(7726)
- By Email
  - support@rsam.com
- Via Portal
  - Request an account via support@rsam.com and then you can create tickets via the portal at https://tickets.rsam.com

- Any errors in the application
- Licensing Questions
- Install Issues
- Performance Issues
- Initial eMail setup / connectivity
- LDAP Connectivity, SSO
- General Issues
- All Rsam customers get a number of designated contacts. Only these contacts can reach out to Rsam support via the channels mentioned prior
- All other organization-members requiring Rsam support should work through their Designated Rsam Contact

The Building Blocks of a GRC Platform

What we Do

Galvanize

Solutions

GRC
(Governance, Risk & Compliance)

Rsam ITGRCBond
Rsam ContinuityBond
Rsam Policy Bond
Rsam IncidentBond

SEC
(Security Operations)

Rsam CyberBond

VRM
(Vendor Risk Management)

ThirdPartyBond

BYO
(Build Your Own Use Case)

Modify Baseline Configuration
Create Custom Solutions

Rsam Platform

Data Architecture	Automation	Business Rules	Content	Reporting	Integration
Homepages	Workflow Roles	Unlimited Rules	20 Managed Domains	31 Native Chart Types	Rsam Universal Connector
Forms	Workflow States	User Defined	11K+ Question Library	Rapid Reports	30+ Predefined Maps
Objects/Records	Workflow Actions	Criteria/Actions	Harmonized Controls	SSRS Advanced Reporting	User-Defined Maps
Relationships	Decision Trees	Computations/Calculations	Active/Archived Libraries	Indicators	Email Listener
Attributes	Notification Templates	Simulations			Rsam RESTful API
Multi-Lingual/Localization	Ad-hoc/Scheduled/Triggered				

What are Rsam Modules?

Baseline Definition

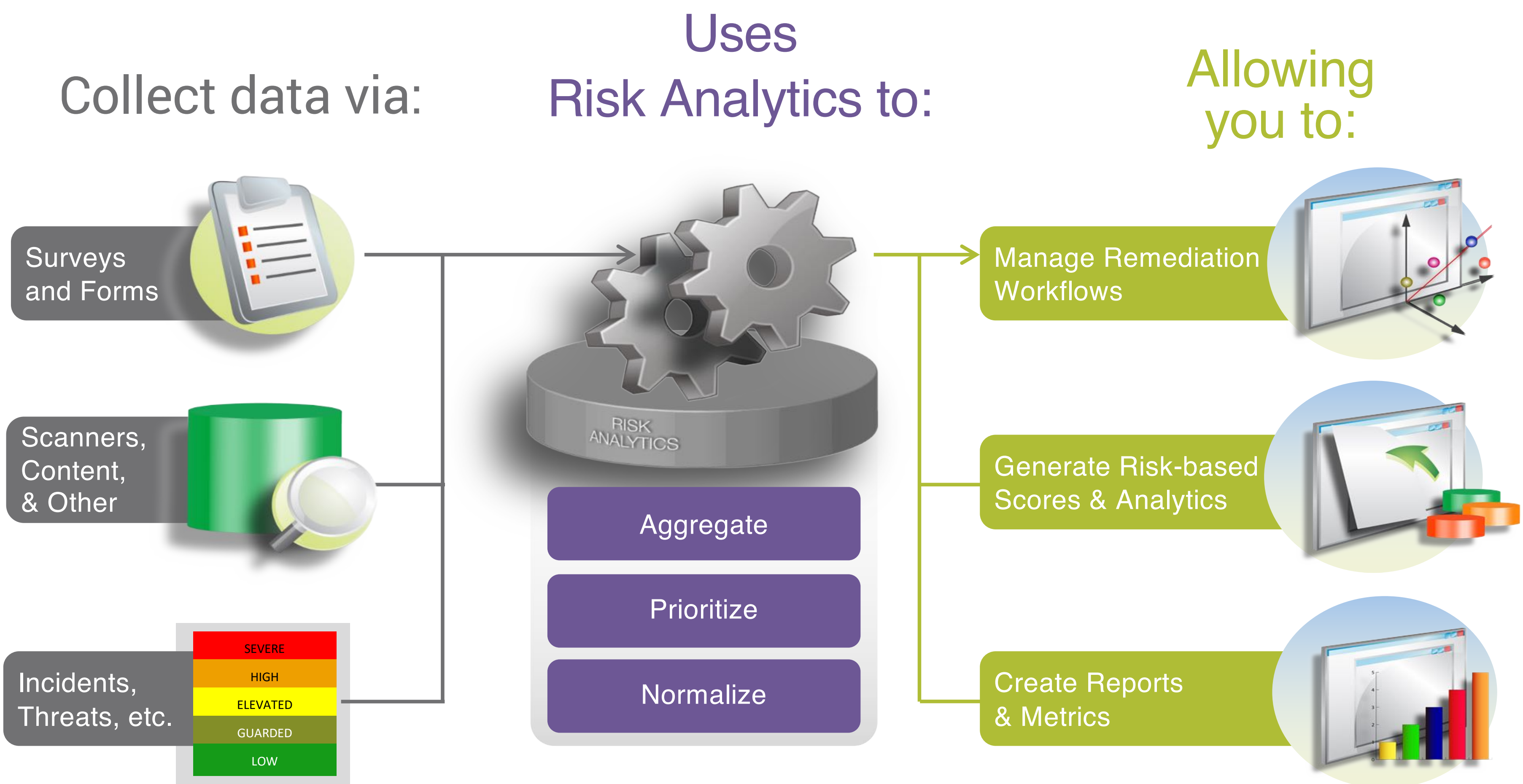
- Pre-defined configuration of various platform elements in support of a defined use-case.

Common Module Components

- Configured Forms
- Content
- Data Connectors
- Defined Data Architecture
- Defined Workflow
- Navigators, Charts, & Reports
- Notifications
- Established Business Rules
- Role-based Homepages
- User Roles

Rsam GRC – How it works

Galvanize



Content

Galvanize

Rsam Managed Content

- 201 CMR 17 - Massachusetts Standards for the Protection of Personal Information of Residents of the Commonwealth
- COBIT - Control Objectives for Information and Related Technologies (ISACA)
- COSO - Committee of Sponsoring Organizations of the Treadway Commission
- CSA - Cloud Security Alliance
- FERPA - Family Educational Rights and Privacy Act of 1974
- FFIEC - Federal Financial Institutions Examination Council
- GLBA - Gramm-Leach-Bliley Act
- HIPAA - Health Insurance Portability and Accountability
- HIPAA HITECH - Health Information Technology for Economic and Clinical Health Act
- and more……

Not a fully official complete list.
This content is used to create:

- Harmonize
- Discreet question sets.

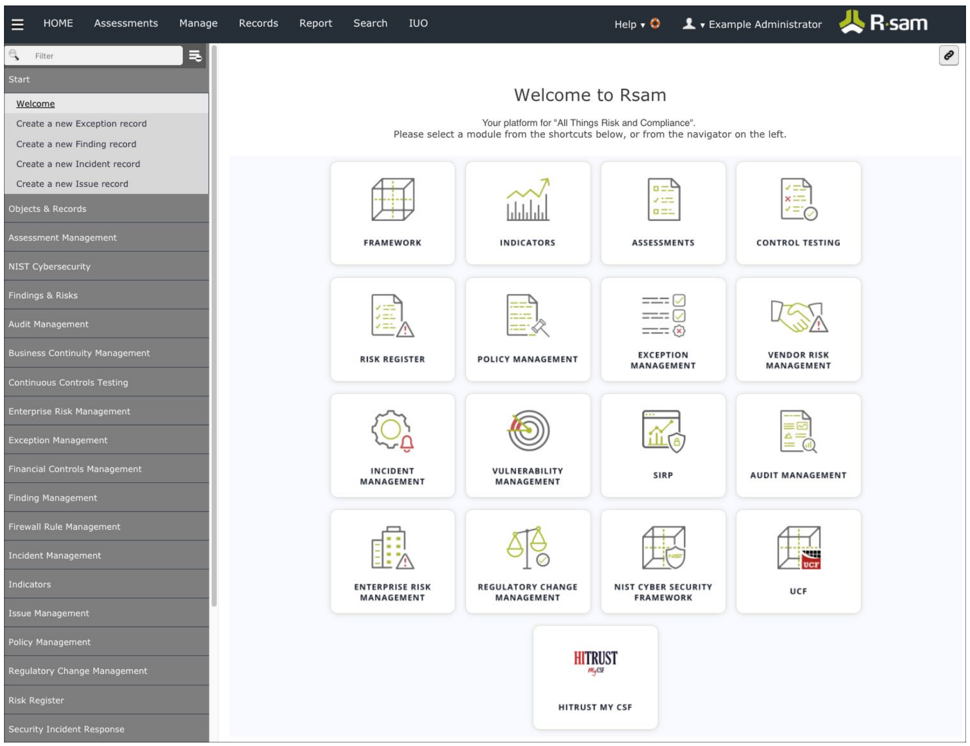
Integration

Connectors - Maps	Connectors - API
Provides pre-built mapping identifiers to support importing of data from various external sources into Rsam.	Provides the ability to pull and push data from/to external systems

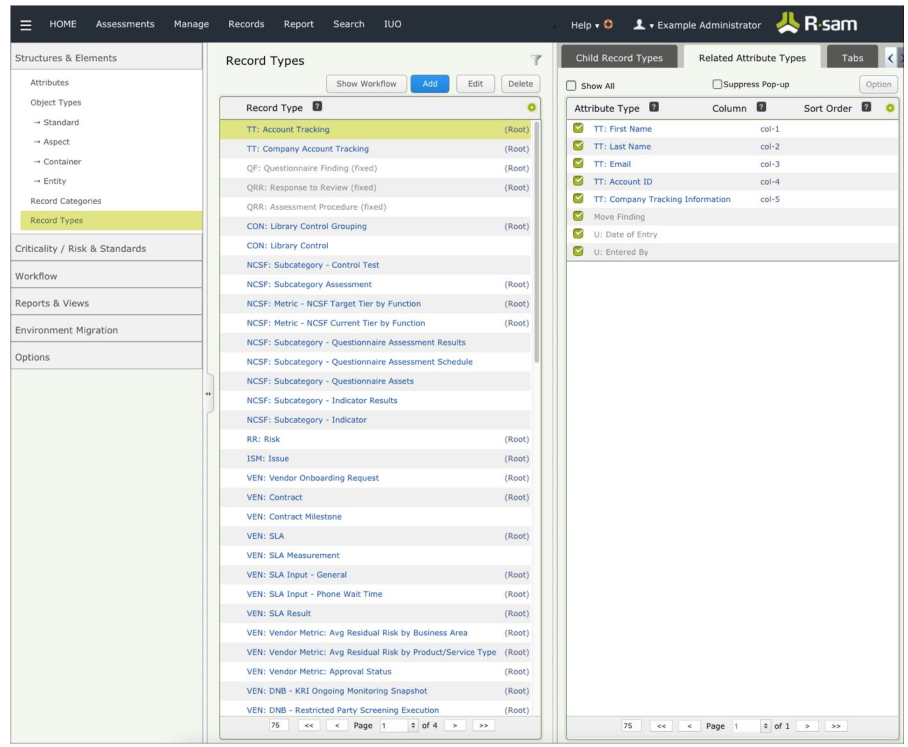
Tour of Rsam

Galvanize

User Interface



Admin Interface



Introduction to Rsam

Learning Rsam

Rsam is a powerful tool that can be as simple or comprehensive as you need

- The following are practical rules to follow:
  - Consider all requirements but do not plan to implement them all right away
  - Identify the most practical / critical one's first. Simple is better.
  - Expand as time progresses

- Keep your implementation as straight forward as possible
  - Configurations and data management should be understood and maintainable (SDLC / SOP)

- Hands-on practice after training is a must
  - Individuals that work with Rsam immediately after training catch on quickly
  - Your cloud instance will remain available for 2 weeks after training

Deploying Rsam

Rsam can scale for Enterprise deployments, as well as for specific point-solutions

- Start simple, no more than 2-3 use-cases for initial deployment
  - Most customers have multiple use-cases for Rsam
  - Start simple and then add more complex use-cases
- As more use cases are implemented, less support from Rsam consultants will be required
- Rsam's goal is to enable customer administrators to be self sufficient
- Updates or new configuration can then be performed with minimal guidance

General Administrative Principles

- Relational Structures
  - Framework is built on a highly relational model. Customers are provided with the ability to use and re-use almost all administrative elements
  - Modules Consists of several pre-defined libraries:
    - Controls, Attributes, Workflow, Handlers, Content etc.
    - Items in these libraries can be shared across all other Rsam modules and BYO
  - Relationships between administrative elements provide a great deal of flexibility and efficiency, but also require extra care on behalf of the Rsam architects & administrators
  - Skills learned from building/managing one Solution are easily transferable to other Solutions in Rsam

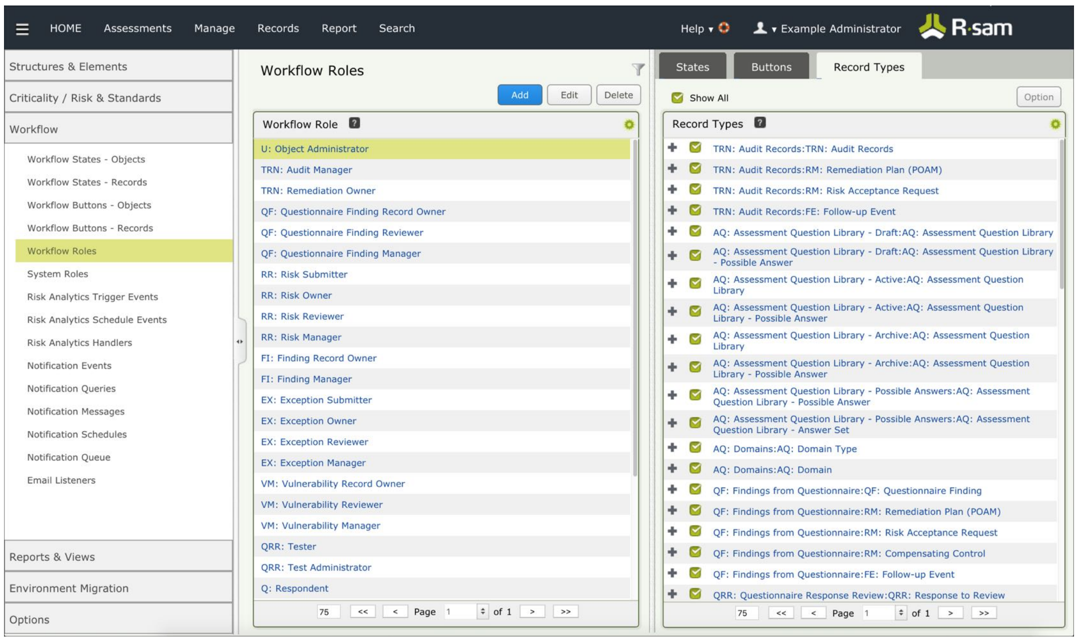
House Keeping

Systems ships with two key accounts

- r_admin (Full access to the system, can do everything)
  - Additional Admin accounts that can be linked to individuals should be created and used.
  - Shared accounts is not a best practice
  - Delete the r_admin account
- Administrator (Has no access to data)
  - Best Practice: The password for this account should be changed and securely stored and used only for recovery purposes.

Administrator Access

- A best practice is to provide the Administrator Roles with access to the data and administrative elements to help with troubleshooting.



- This approach is a good idea in Development / Test Environments
- This approach should be reviewed for Live Environments
  - Ideally it should be a business decision

Browser Notes

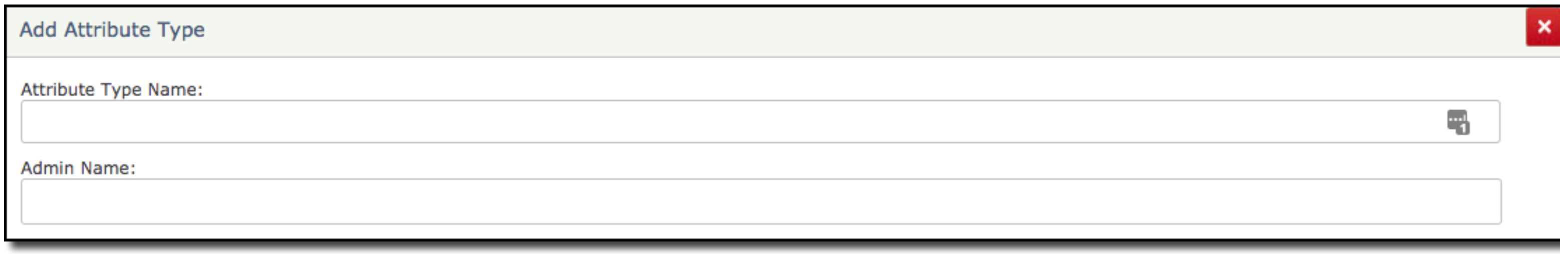
- Supported browsers include

Safari Firefox chrome Internet Explorer

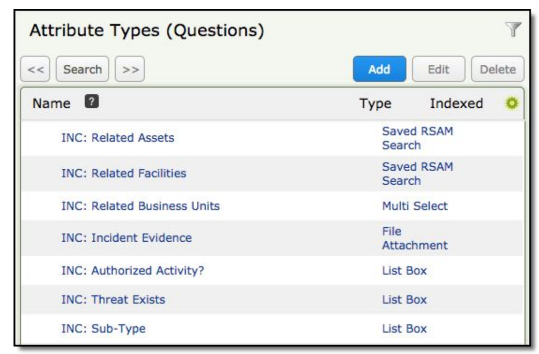
- Use of back button will cause issues (connection with SQL)
- Best Practice:
  - Use two independent browser types
    - 1 for admin (Chrome) & 1 for User Testing (Firefox)
  - Use two different instances under one browser (incognito mode, private mode)

Naming Guideline

Most items in Rsam have a “name” and an “admin name”

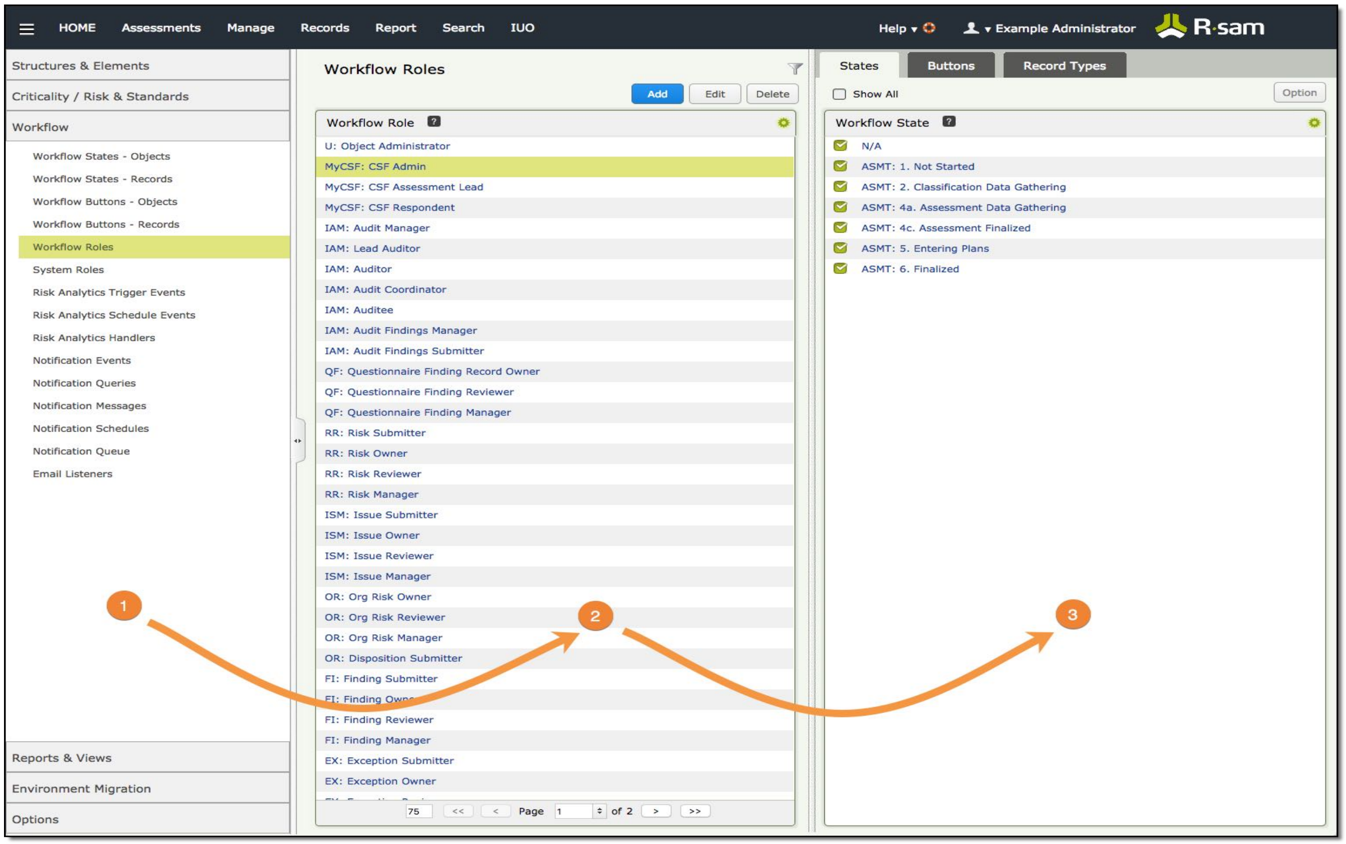


- The Name is what the end user will see
- The Admin Name is what Admins see when configuring items
  - Prefix the admin name with something relevant
  - Use this prefix to define what you created
  - This will help with day to day and long term management of your environment
  - Advanced techniques allow you to group and sort on the prefix



Linkage

- Every Administrative Element in Rsam needs to be configured for items to appear / work.

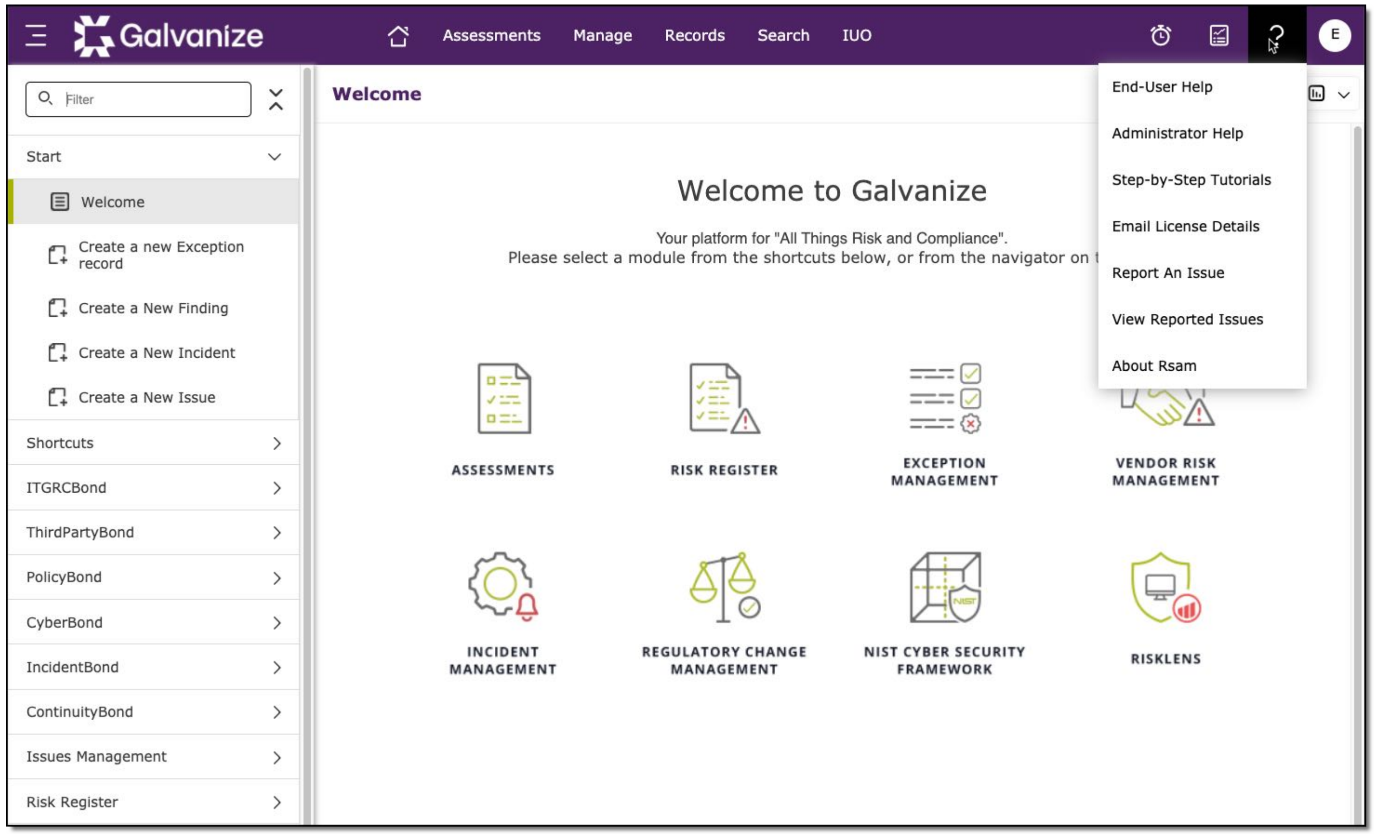


As you select items on the:

1. Left hand windowpane
2. Options will appear in the middle windowpane
3. and then in the right windowpane that will require/allow you to configure relationships.

Help Options and Versions

- End User Help
- Administrator Help
- Step by Step Guides
- Email License Details
- About Rsam



Galvanize

Structures & Elements Overview

Learning Objectives

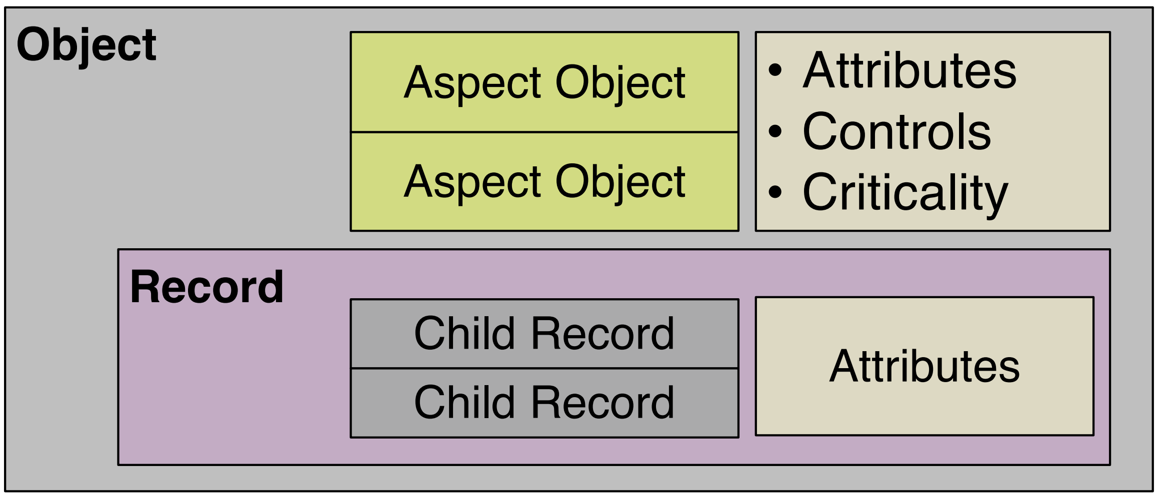
Galvanize

- At Completion of this Section you will:
  - Understand and be able to identify the foundational components of structuring data within Rsam
  - Understand the use of Objects
  - Understand the use of Records
  - Understand the role Attributes play with Objects and Records

Objects & Records

Galvanize

- **Objects** & **Records** provide the foundation for structuring data inside of Rsam. The following images represent the basic Rsam structure covered in the following slides



Objects

Galvanize

Objects hold and organize information in Rsam

- Objects can be tangible (such as a Vendor or Application) or intangible (such as Libraries, Departments or Processes)
- Objects are a great mechanism to group together data across modules, and provide a logical point of navigation, reporting, and permission assignment
- Objects can hold many things within them, most commonly:
  - Attributes to describe the object itself
  - Control & Criticality questions to assess the Object
  - Records to track and manage rows of data within the Object

Records

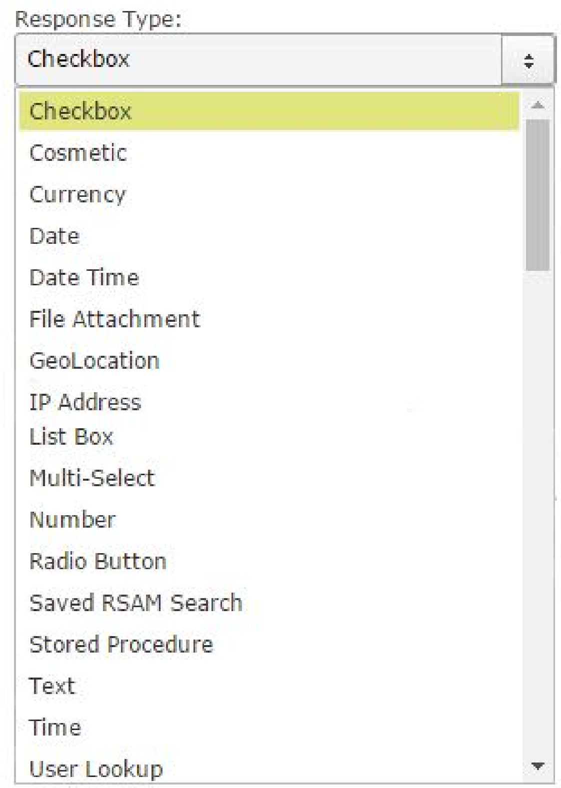
Records are thought of as individual rows of data that are used to track, manage, and report on information within an object

- Records exist within objects (tangible & intangible)
- Records provide the simplest method to track rows of information, similar to data from Excel, a database or other applications
- Records can leverage all advanced features including workflow, handlers, import, etc

Attribute Types

Attributes are used throughout Rsam to record information for Objects & Records

- For Records, all data is stored in Attributes
- For Objects, Attributes are typically used to store “descriptive” data
- Attributes do not contribute to Rsam’s out-of-the-box assessment scoring system
- Attributes can be used extensively for filtering, grouping, and sorting data in Rsam
- Attributes can be hidden for use in data calculations or displayed only when needed



Galvanize

Structures & Elements

Records

Learning Objectives

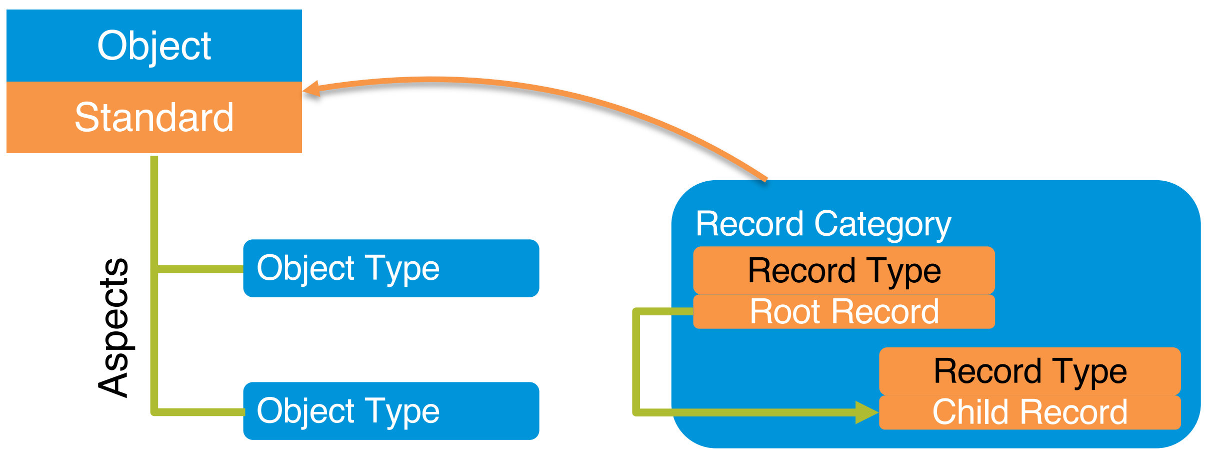
- At Completion of this Section you will:
  - Understand the use of Record based solutions
  - Understand and be able to identify the components of a Record based solutions
  - Understand the use of different types of Records

Rsam Terminology

	Technical	Non-Technical
Record Category Type	Creating a Database	New Excel Spreadsheet
Record Type	Creating a Table	Sheet within an Excel Spreadsheet
Attribute	Field in a Table	Column within a Sheet
Record	Row in a Database	Row within that Sheet
Saved Search Attributes	Lookup Queries to other Databases or Tables	Look up on another Tab

Records

- Records reside within Objects
- Records represent individual items containing information such as:
  - Individual Gaps, Audit Findings, Vulnerabilities, Remediation Plans & more
- Records are light-weight and simpler compared to Objects



Creating Categories

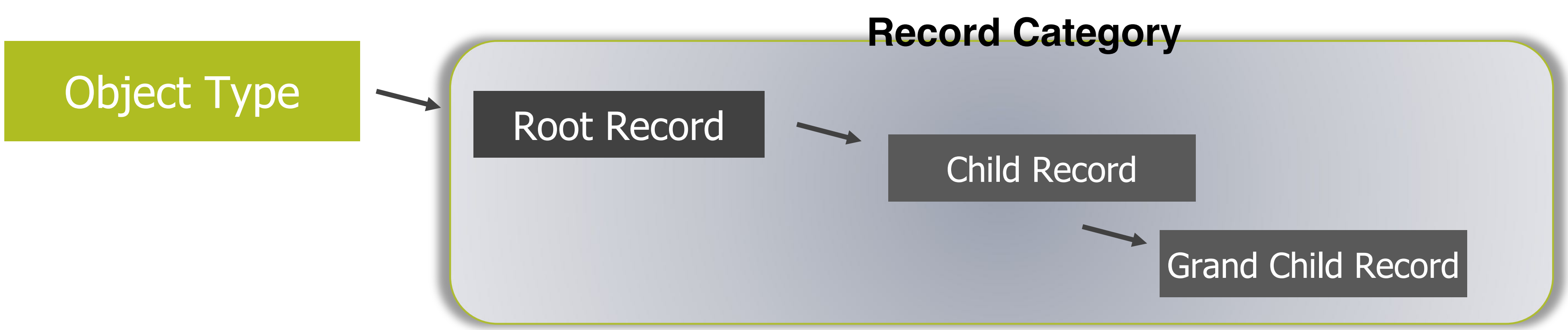
Record category Types define the highest grouping in the Records structure. Categories classify the various uses for Records

- Categories hold one or more record types
- Categories can be assigned to one or more object types
- Administrators can specify a default object for a record category
  - Records within that selected category will always default to the selected object
  - Other screens (like import, etc) will default to this object

Creating Records

Record Types define the individual configurations in the Records structure Record Types can be designated as root, or child, and can be structured into a multi-level hierarchy

- Root Records can have multiple child records
- Child Records can have their own child records
- Record Types use attributes to hold all data related to the record



Galvanize

Creating Record Categories & Types

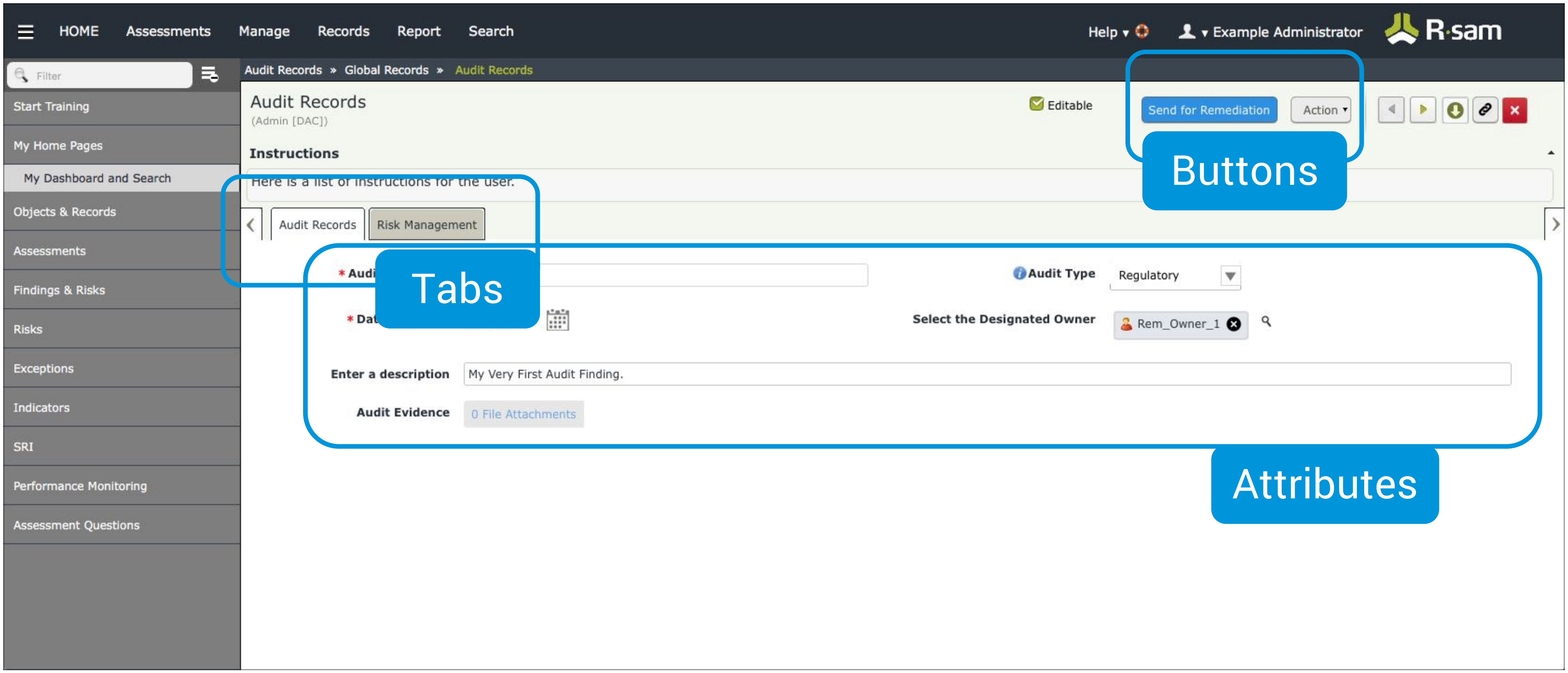
Exercise

What are we going to build?

- Our example is going to walk you through building a solution from scratch.
  - Creating a Record Category
  - Creating a Record Type
  - Linking to an existing Object
  - Creating Attributes
  - Creating Accounts & Assigning Permissions
  - Creating Workflows, Buttons and Risk Analytic Handlers
  - Creating Risk Analytics
  - Importing Data
  - Building Searches
  - Creating Home Pages
- These tutorials will allow you to build skills that can then be used on your own solutions or with the Modules that you may have purchased.
- Along the way we will show you different elements that can be configured to provide alternative views to the end user.

What are we going to build?

Galvanize



Galvanize

Administrative Groupings

Learning Objectives

- At Completion of this Section you will:
  - Understand the purpose of Administrator Groupings
  - Identify who can create Administrator Groupings
  - Be able to implement Administrator Groupings

Administrative Groupings

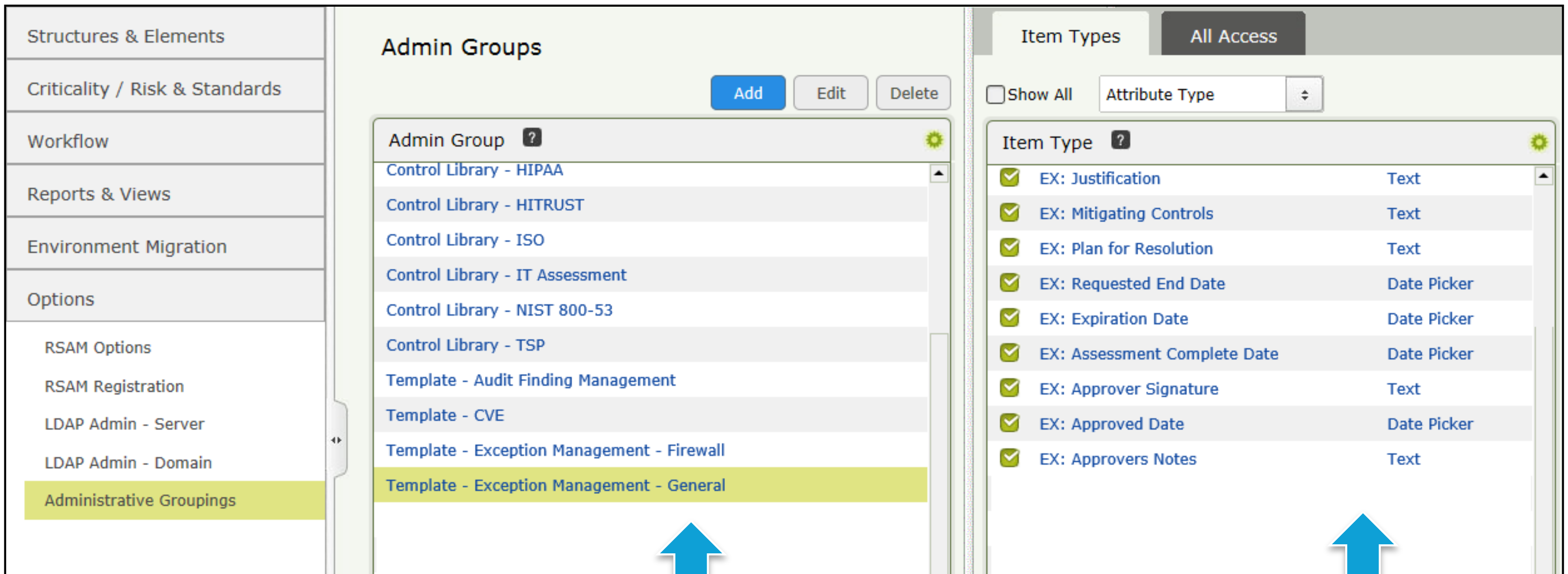
- Administrative Groupings allow grouping together multiple administrative elements, making administration easier by:
  - Allowing administrators to filter their administrative screens by one or more Administrative Groupings
    - EXAMPLE: “Incident Management” configurations can be viewed and managed without displaying the “Vulnerability Management” configurations.
  - Allowing administrators to assign portions of the administration to different users based on their System Roles
    - EXAMPLE: Manage which Rsam users can read, modify, add, delete “Incident Management” configurations vs. “Vulnerability Management” configurations
  - Making it easier to manage Environment Migration Selections, discussed later in this course

Administrative Groupings

Galvanize

- Administrative Groupings are configured under the Options menu in Rsam's Administration Screens
- Only Data Administrators or Account Administrators can create administrative groupings
- Groupings can be associated with "Individual Administrative Items", e.g., individual attribute types.
- Groupings also have options for "All Access", which allow you to include "all attributes, all control, etc" in the group.
  - NOTE: This multi-select environment allows you to select many administrative items and checking them all at once.

Administrative Groupings

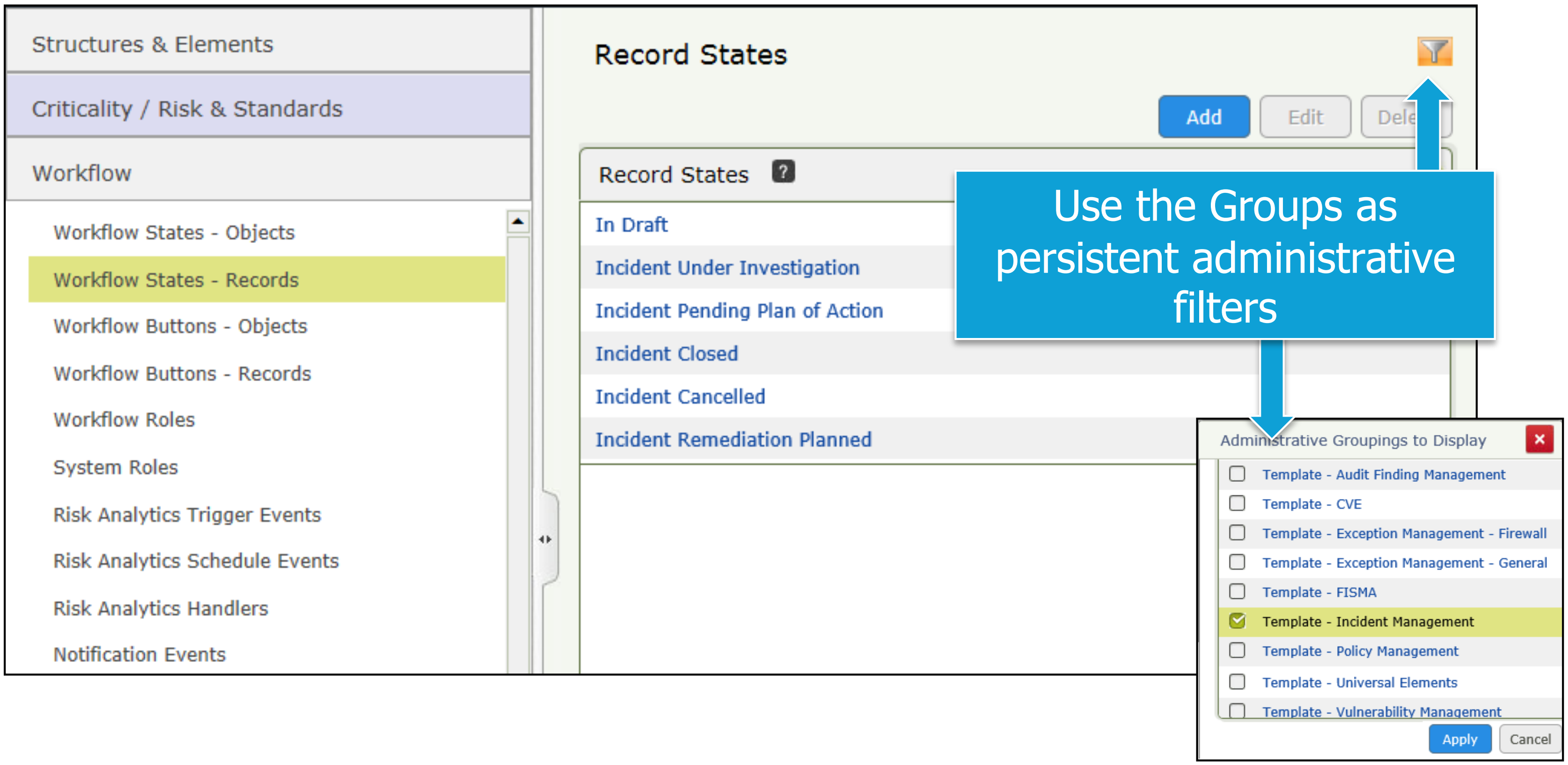


Create Administrative Groups

Associate the Groups with Administrative Items

Administrative Groupings: Filtering Views

Administrative Groupings can be used to filter Rsam Administration screens via the Filter icon



Administrative Groupings: Filtering Views

- While filtering by a single administrative group, any new items added will automatically be placed into that administrative group.
- To easily maintain administrative groupings, it is recommended to always select a single filter before adding new elements.
    - EXAMPLE: if you are filtered by the “Vendor Management” group, and you add in a new attribute type in the attribute type screen, that new attribute type will automatically be placed in the Vendor Management group.

Administrative Groupings

Exercise

Galvanize

Structures & Elements

Attributes

Learning Objectives

- At Completion of this Section you will:
  - Understand the purpose and use of Attributes for Record Based Solutions
  - Understand configuration options for Attributes
  - Understand key features of Attributes
  - Identify where Attributes are placed

Attributes

Attributes define the individual fields of data that can be entered for each Record

  - (e.g.; Text, Data, File Attachment, List Box, Check Box)

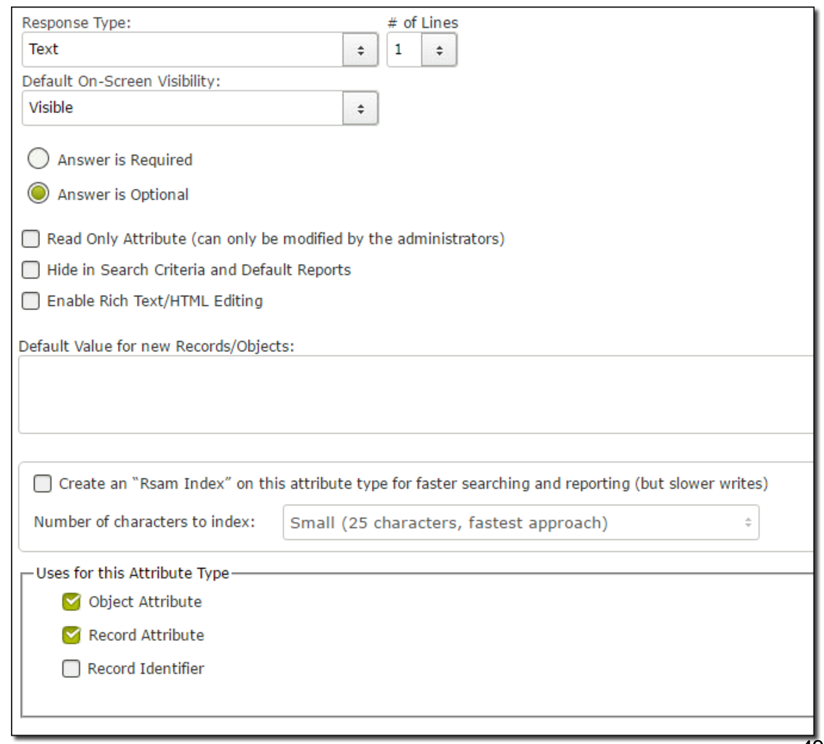
- Create an Attribute Type for each field of data to be recorded
- Attribute Types are created in the Administration Screen
- To use an Attribute with Records, check the Record Attribute option when making the Attribute Type and relate the Attribute Type to the Record Type

Common Attribute Type Settings

Galvanize

Attribute Types have several settings that can apply to most of the Response Types

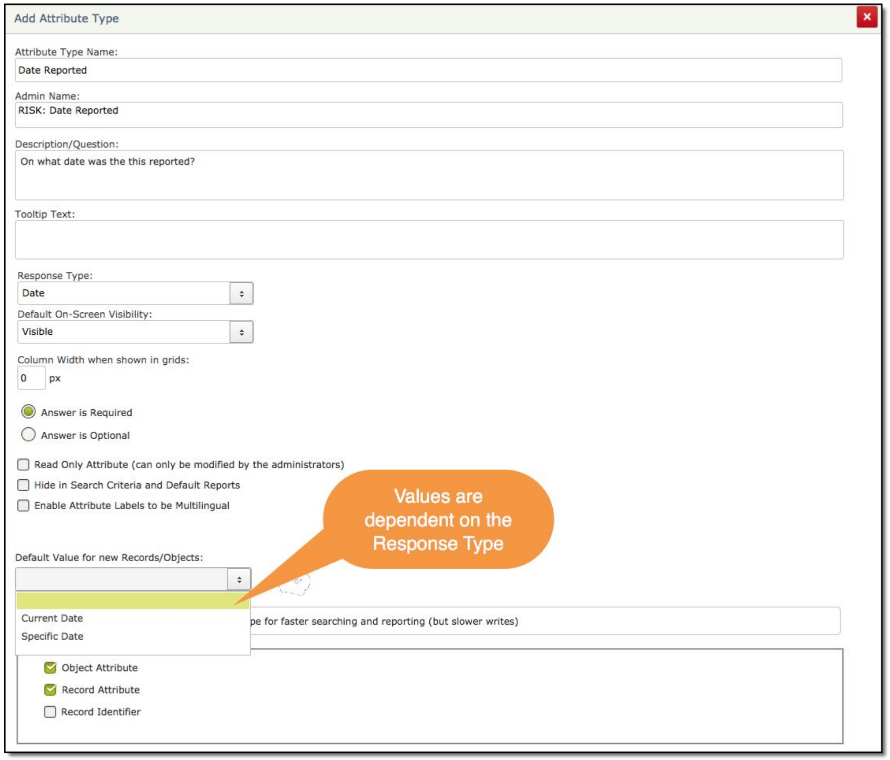
- Visible or Hidden
- Required or Optional setting creates a visible cue for the user *
  - Handlers are needed to force the user to enter a response, when needed
- Read Only Attribute
- Hide in Searches/Reports
- Enable Rich Text Editing
- Default Value for new Record/Object
- Create an "Rsam Index"
- Uses for this Attribute Type
- Record Identifier



Default Values for Attribute Types

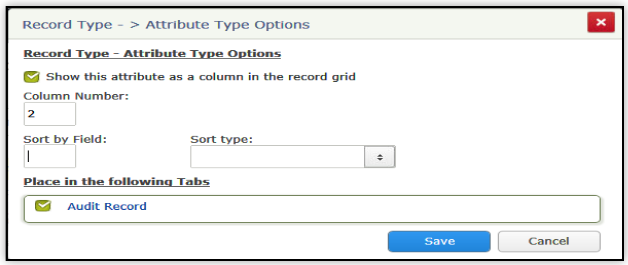
Rsam includes the ability to specify a default value for each attribute type without having to write handlers. For example: Date Created, Created By, etc.

- Eases the administrative burden
- Better performance than using on-create handlers



Creating an Attribute Type

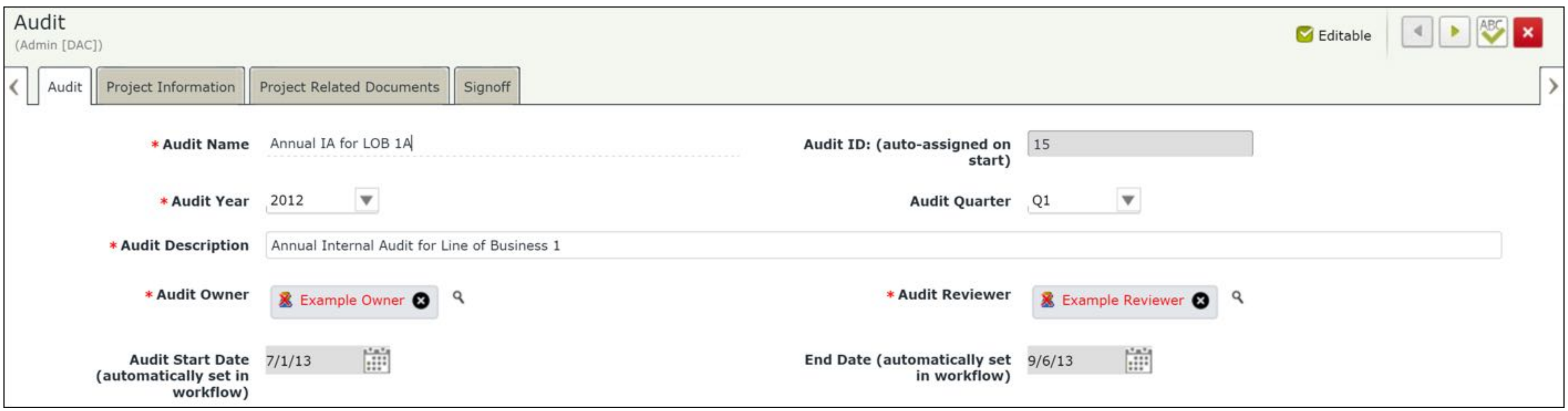
- When relating a Record Type to an Attribute Type, you will see the option to: show the Attribute as a column in the grid



- This allows users to see the data instantly without having to actually open the Record. You may specify the column order for these Attributes

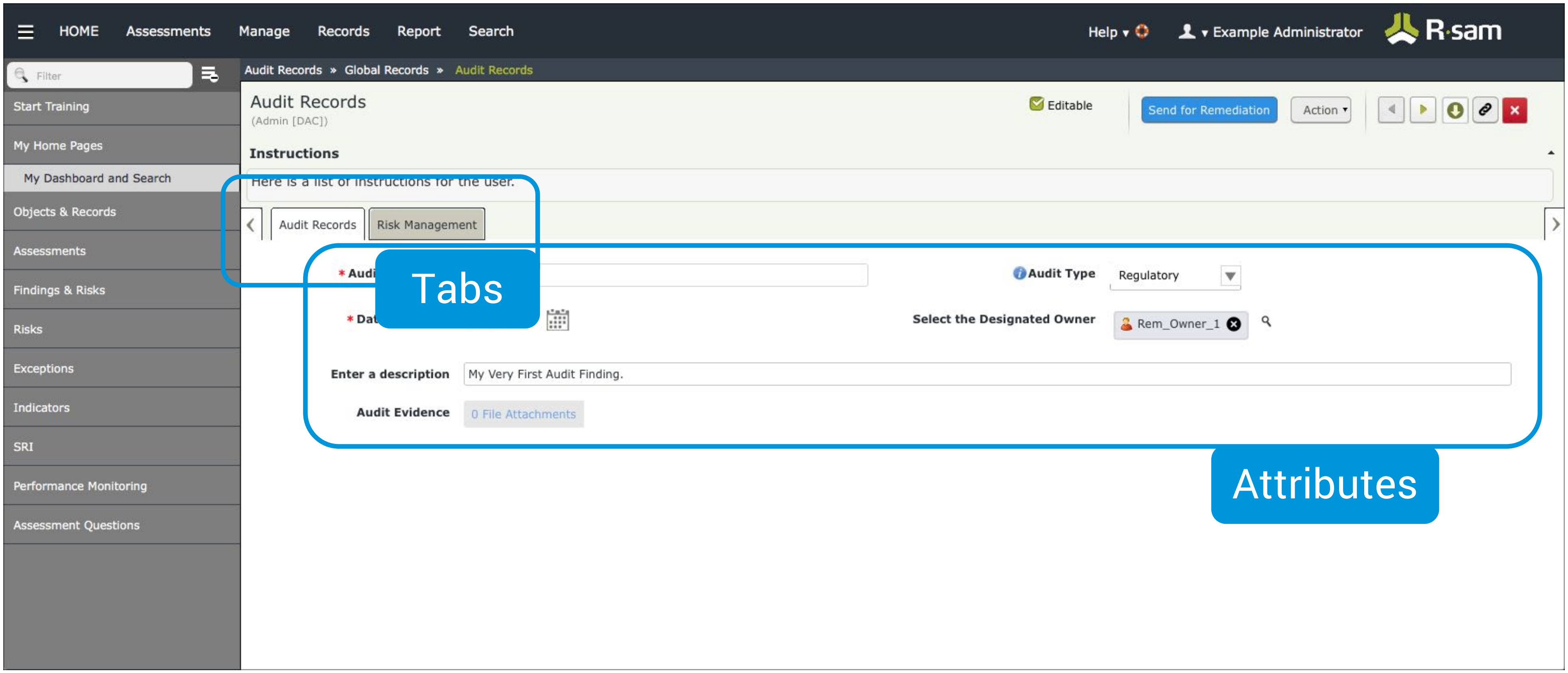
Record Tabs

- Attributes are arranged into Record tabs.
  – Rsam includes a drag & drop interface to arrange Attributes within any given tab
- Access can be assigned to tabs individually giving users with specific roles access to specific tabs



What are we going to build?

Galvanize



Creating Attributes & Additional Tabs

Exercise

Galvanize

Roles & Permissions

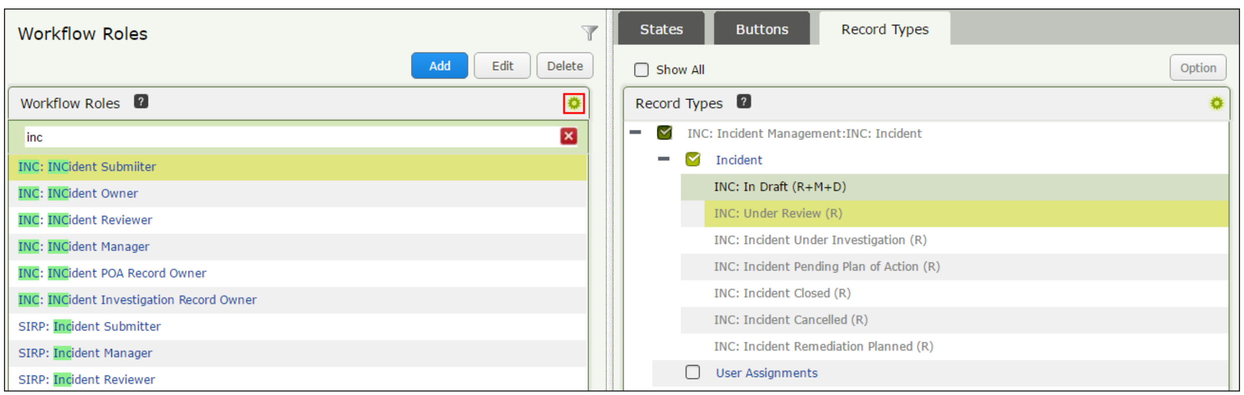
Learning Objectives

- At Completion of this Section you will:
  - Understand the purpose of roles & permissions
  - Understand where and how permissions are assigned to Records
  - Identify where and what Roles can be related to
  - Identify where Attributes are placed

Permissions for Records

Record access is completely driven by user role assignment

- Roles can be assigned to Users or Groups
- Roles define what Users and Groups can see and interact with
- Roles can be assigned directly to a Record, to the Record's parent, and even to the Object or Entity above the Record. All such cases would grant your users access.
  - Tabs: Roles can be associated with specific tabs within the Records interface. This gives the ability to isolate which Attributes the user will have ability to access

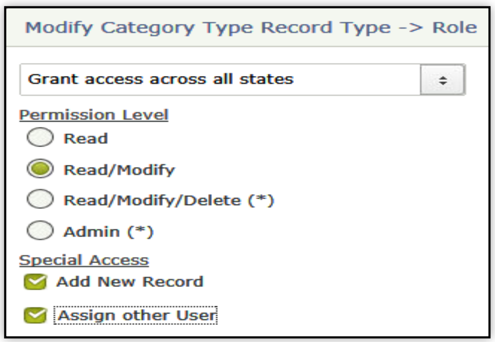


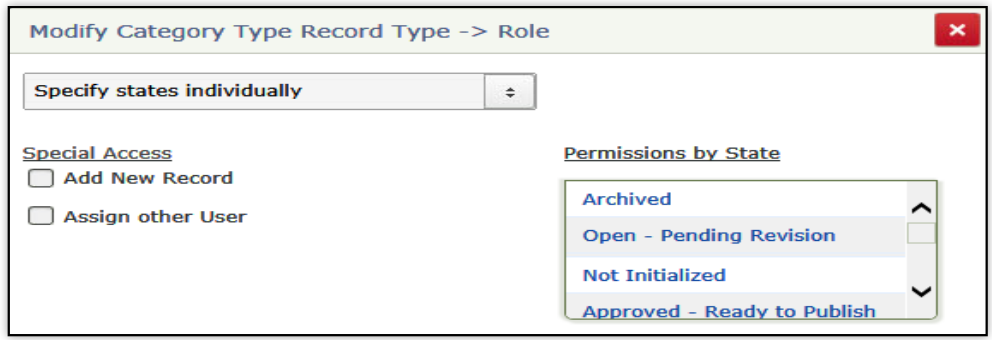
Assigning Permissions

Galvanize

You may assign Records to users across the organization

- Permissions are assigned to Records via Workflow Roles
- When associating a Workflow Role with a Record Type, or a Tab within a Record Type, Rsam will present the following permission options



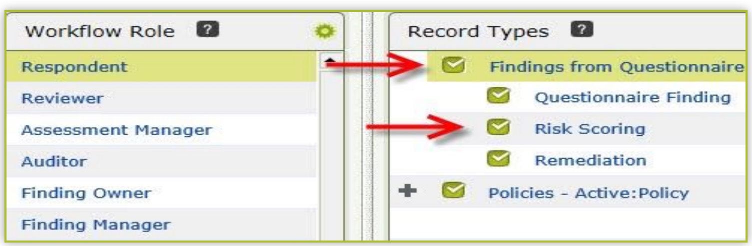


- The selected permission will apply only to Records of that specific Record Type
- Customers can also choose to vary access to the record based on specific workflow states

Assigning Permissions

Roles can be related to the following items:

- An entire record type (most common): Thereby granting access to the entire record and all of its tabs
- Specific record “Tabs”: Thereby granting access to individual tabs and their related attributes
- Specific record “Tabs” within specific “Workflow States”: Thereby granting access to individual tabs, but only while the record is in a specific state



Assigning Permissions

Permissions may be assigned in 3 places:

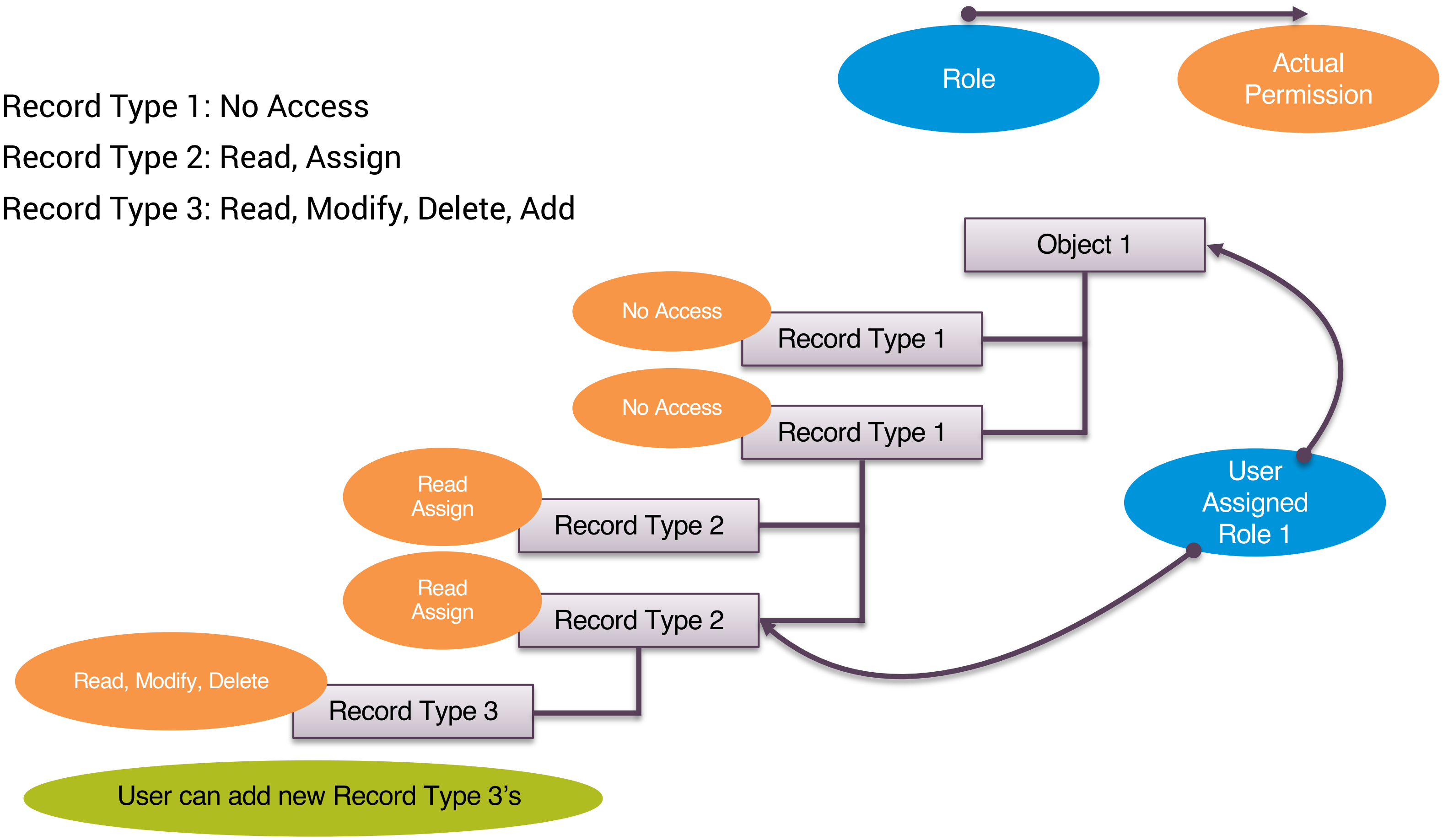
- Object Level:
  Assign a user or group a role to an entire Object, Sub-Entity, or Entity. In this case, the user will have that same role for all Records within the designated Objects
- Parent Level:
  Assign a user to a Parent Record. In this case, the user will be given the role to that Parent and of its Children, etc.…
- Individual Record:
  Assign a user to an end-node Record (no Parents). In this case, the user will be given that role for only that individual Record
- Important: Even if the user is assigned a role to many Records, if that role has not been associated with that Record Type, the user will have no access to it

Permission Assignment Examples

Galvanize

Scenario

- Role 1: Record Type 1: No Access
- Role 1: Record Type 2: Read, Assign
- Role 1: Record Type 3: Read, Modify, Delete, Add



Permission Caution

Galvanize

Permissioning of users is very powerful

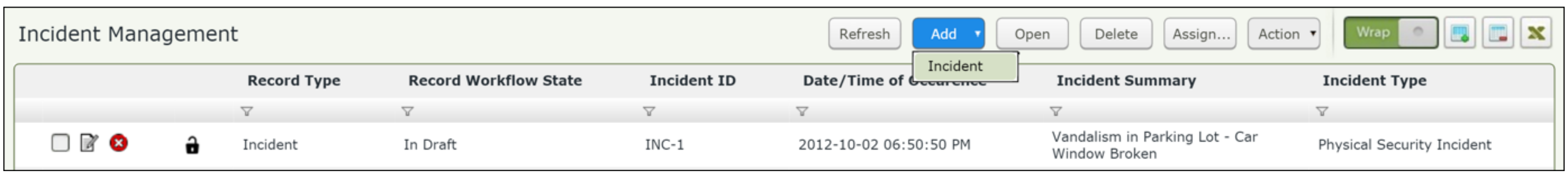
- For Baseline: where possible use the out of the box models (documented in baseline guides)
  - This provides a high level of Security
  - Provides little to no Redundancy
  - Simple to Manage and Maintain
- For Build Your Own:
  - Consider working with Rsam
  - This will ensure a high level of Security
  - Limit Redundancy
  - Keeps the system optimized

Using Records

Galvanize

Records are accessed from many screens in Rsam.

- Records can be created:
  - Manually from the Record Grid
  - Via Self Registration
  - Via Data Import
- Click on Add to create a Root Record
  - Below is an example of adding a new record



- If the Record has associated Child Record Types, you may also choose to add one or more Children

Creating & Assigning Accounts, Roles & Permissions

Exercise

Galvanize

System Roles

Learning Objectives

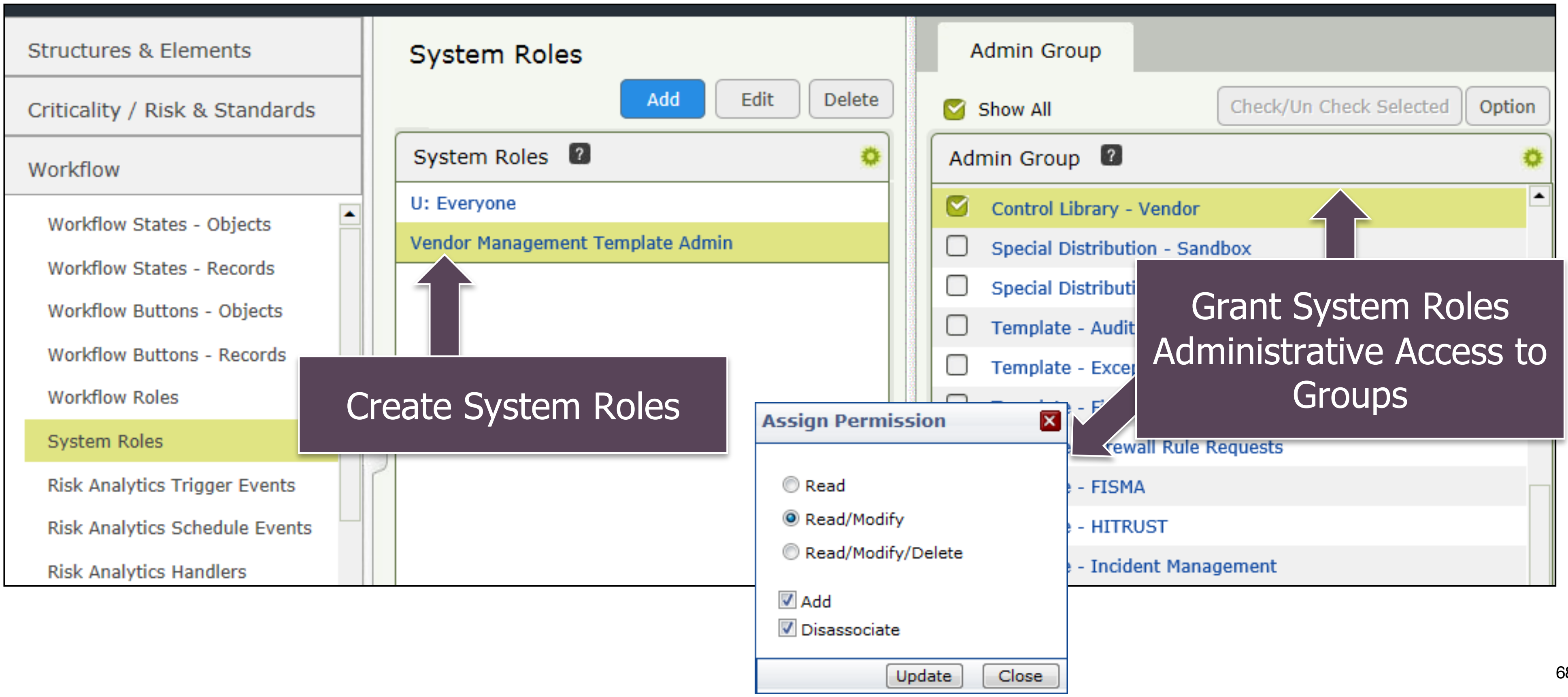
- At Completion of this Section you will:
  - Understand and use System Roles to parse out admin tasks to users who do not have specific admin privileges

System Roles

- System Roles allow administrators to assign users / groups directly to system-level roles for specialized uses.
  - System roles allow access to specific administrative screens / items by associating the role with one or more administrative groupings.
  - System roles allow access to home screen tabs
  - System roles are assigned directly to users / groups in the Manage Users/Groups screen
  - System roles do not automatically provide access to the data

System Roles: Assignment of Admin Group

Assign administrative groups to system role to allow for limited administrative



Creating and Using System Roles

Exercise

Galvanize

Users & Permissions

Learning Objectives

- At Completion of this Section you will:
  - Understand the different User account types
  - Identify the different access control types
  - Understand the different ways users can be created
  - Identify where permissions can be assigned
  - Understand how user permissions function

Account Types

While user permission assignment determine a user's object & record permissions, each user has an account type to designate administrative access:

- Standard User: This is the default for all users. Standard users have no access to the Rsam administration screens
- Data Administrator: These users have access to the Rsam administrations screens, all objects and all records
- Account Administrator: These users have full Data Administrator access, as well as the ability to designate other users as administrators, and create internal Rsam accounts (non-LDAP accounts)

Rsam User Architecture

Access Controls allow you to assign permissions and roles to individual users or groups

- Rsam includes features to fully integrate with LDAP directories, Active Directory, Single Sign-on, and more
- In Rsam customers can define:
    - Users and Groups
    - Workflow Roles
    - System Roles

Creating Users

Users can be created via the following mechanisms

- Transparent: Assigning an LDAP user to a record or object will automatically create the required elements for the user to access Rsam
  - There is no need to create individual user accounts
- Manually Importing users from an LDAP source
- Manual Creation of an Rsam (non-LDAP) users
- Enabling User Self-Registration

User Self-Registration

- Self registration can be enabled for “Internal” and/or “External” users
  - Internal users must have an existing LDAP account
  - External users do not require an LDAP account
- Optional: Self registered user accounts can be set as pending, requiring approval before using Rsam

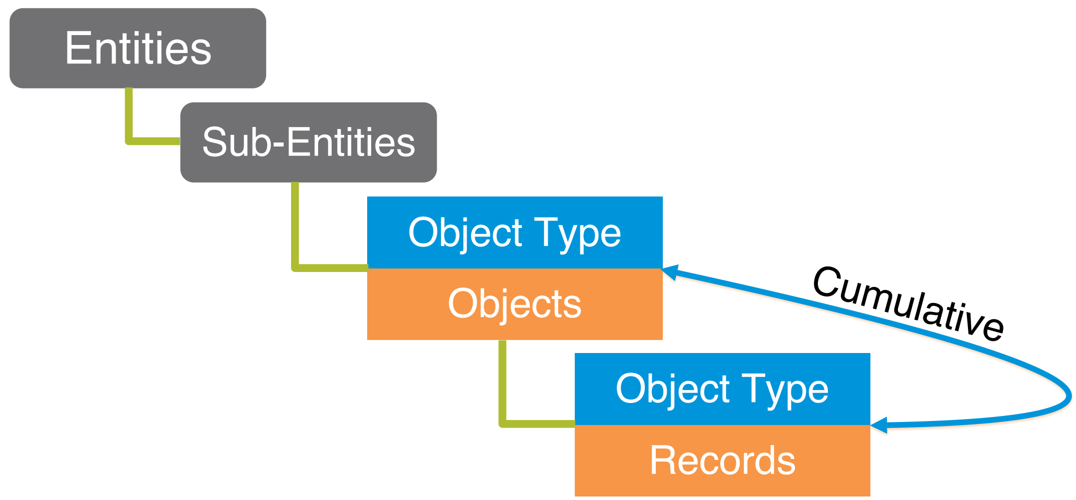
Assigning Permissions

Users can be assigned permissions to access objects & records via the following mechanisms:

- Assignment Via Attributes: Administrators can configure attribute to auto-assign a role to users selected as the attribute response
  - This is the most transparent method of assigning permissions
  - This is also highly useful if you want to import user assignments from Excel or another data source
- Direct Assignment: Users with user assignment privileges can choose to check on the “Assign other user” button and select the user from the User Search screen. This is available on most object & records screens
- Permission Manager Screen: Administrators can assign many permissions at once by using the Permission Assignments Screen

User Privileges

- Users can be assigned privileges directly or by being a part of a group
- Privileges may be associated with an individual object or all objects within an entity
- Privileges are cumulative, so all permissions are combined for each user



Performance Caution

Galvanize

- Rsam supports the ability to assign individual users to individual records, allowing customers to possibly set hundreds of thousands of permission assignments
  - Such practices, however, do have an impact on performance
  - When assigning users, try to assign at the highest acceptable level
  - Assigning a user to an object that has 10,000 records yields far better performance than assigning the same user individually to each of the 10,000 records
- Rsam allows for complex role assignments where customers can specify which roles can access which tabs of a record type and can vary that for each workflow state
  - While this is a powerful feature, we recommend limiting the user of role -> record type -> tab -> workflow state assignments as this:
    - Can lead to redundant permission (potential for huge performance hit)
    - Becomes a challenge to manage
    - Can also lead to slower performance if not kept under control

Galvanize

Workflow

Learning Objectives

Galvanize

- At Completion of this Section you will:
  - Identify the different workflow components
  - Understand the use of each workflow component

Dynamic Workflow

Workflow determines the way in which each Object or Record progresses.   They can be simple and direct, or rich and elaborate

Rsam includes pre-defined workflows

- Clients may create their own custom tailored workflow using the following components
  - Workflow States: Define the current position of an Object or Record within the use-case process
  - Workflow Roles: Are a mechanism to assign users to perform certain tasks with an object or record depending on its current state
  - Workflow Buttons: Mechanisms primarily used to advance an object or record from one state to the next. Buttons can also be used to have various effects, trigger e-mail notifications, display on-screen data, or triggering Risk Analytics handlers

Workflow States

States represent the different parts of the workflow in which an Object or Record can reside

- At any point an Object or Record is in a single Workflow State
- States determine:
  - Who can access the item
  - What the user should be doing with that item
  - What buttons / actions are available
- Searches and Dashboards can be filtered by workflow states, making it easy to build work queues
- Risk Analytics can use workflow states as criteria to trigger automated actions

Workflow Buttons

Buttons represent the interface element the users can click for their assigned Objects and Records

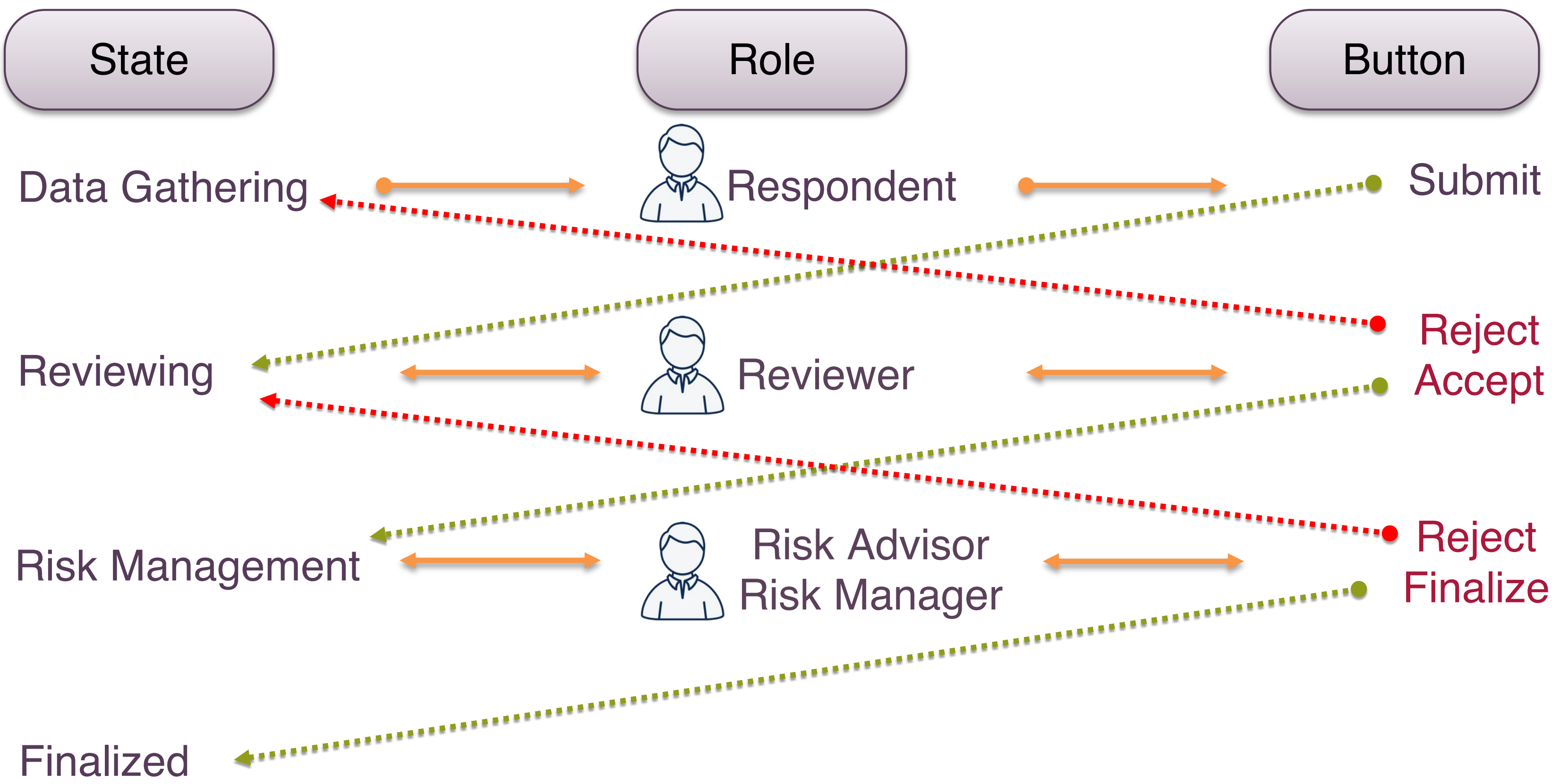
- Buttons are typically used to progress Objects and Records through the various states
- Buttons can be set to:
  - Change the Workflow State
  - Send notifications
  - Prompt for comments / clarifications
  - Compile gaps / records
  - Trigger custom handlers (risk analytics) & more
- Buttons are associated with Workflow States, Roles, and Object Types / Record Types to determine who can click them, when they can be clicked, and for which targets
- Rsam can be configured to automatically “click” buttons

Workflow Roles

Roles represent the part a user plays in the workflow of the Object or Record.
To participate in the Workflow a user must be assigned at least one role to their Records or Objects

- Roles determine:
  - What home-screens the user sees
  - In which states an Object or Record can be accessed
  - What access the user has to Records
  - Which buttons the user can click on
  - What email notifications the user receives
  - What other roles the user can assign & more
- Roles are associated with Workflow States, Buttons, Record Types, Notifications, and more to determine where and how a role interacts with Rsam

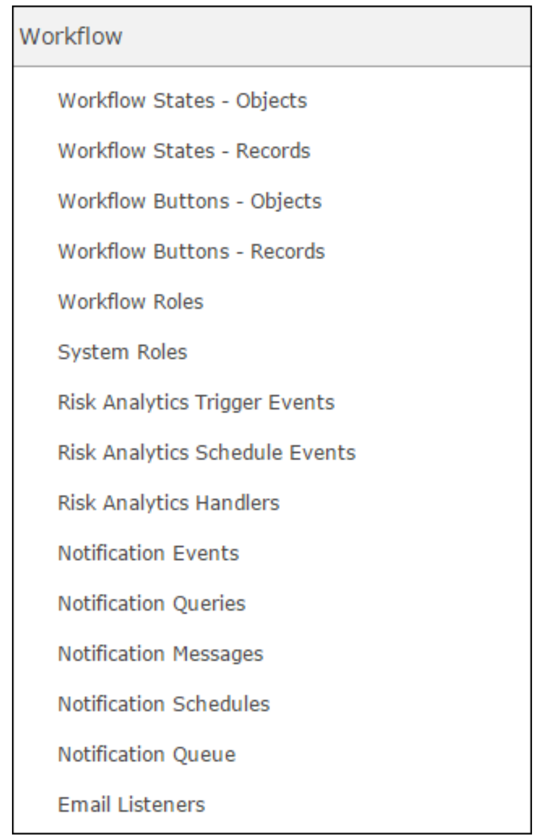
Object Going Through a Questionnaire Process



Other Workflow Elements

Beyond States, Roles, and Buttons, Rsam's Workflow also consists of the following elements:

- Risk Analytics for custom handling of events in Rsam
- Notifications Tasks
- Email Listener for Notifications, Alerts and Reminders



Galvanize

Risk Analytics

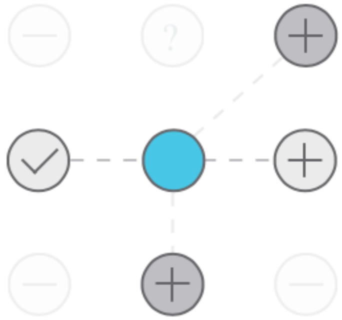
Learning Objectives

- At Completion of this Section you will:
  - Understand the purpose and use of Risk Analytics
  - Identify how to build Risk Analytics
  - Understand the importance of Scope for Risk Analytics

Risk Analytics

Risk Analytics provides the ability to automatically perform actions on both Objects and Records based on customizable criteria

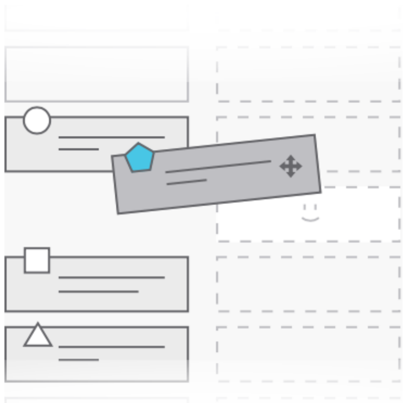
- Risk Analytics is commonly used to automatically:
  - Restart old completed Workflows & expire temporary approvals
  - Adjust a Workflow based on specific responses / values
  - Email users of upcoming & overdue tasks based on criteria
  - Perform calculations for scoring or statistics
  - Escalate critical issues & automatically set due-dates
  - Randomly select items for follow-up testing



Mechanisms of Risk Analytics

Risk Analytics utilizes the following mechanisms:

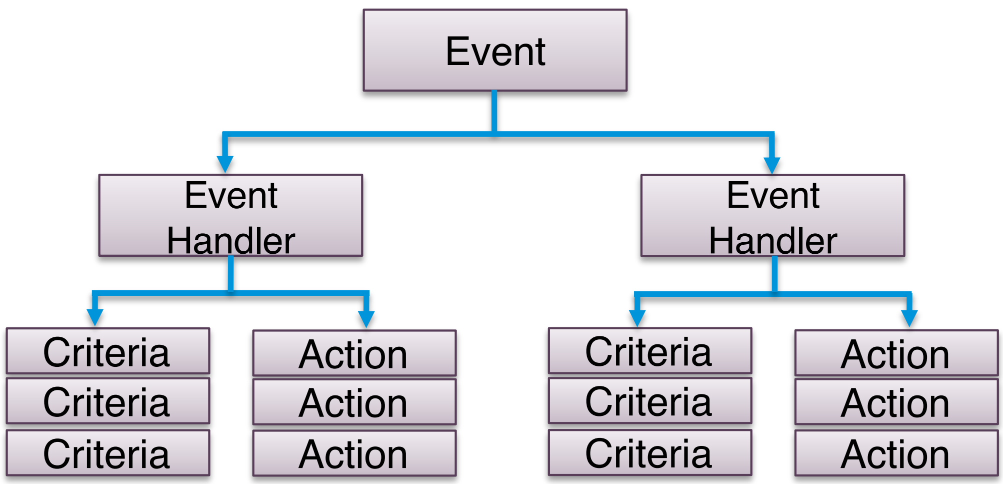
- Events: Represent events occurring in Rsam that can trigger risk analytics including:
  - Clicking on a Button (manually or automatically)
  - Scheduled events that occur automatically on a scheduled basis
- Handlers: Define how Rsam should “handle” specific events



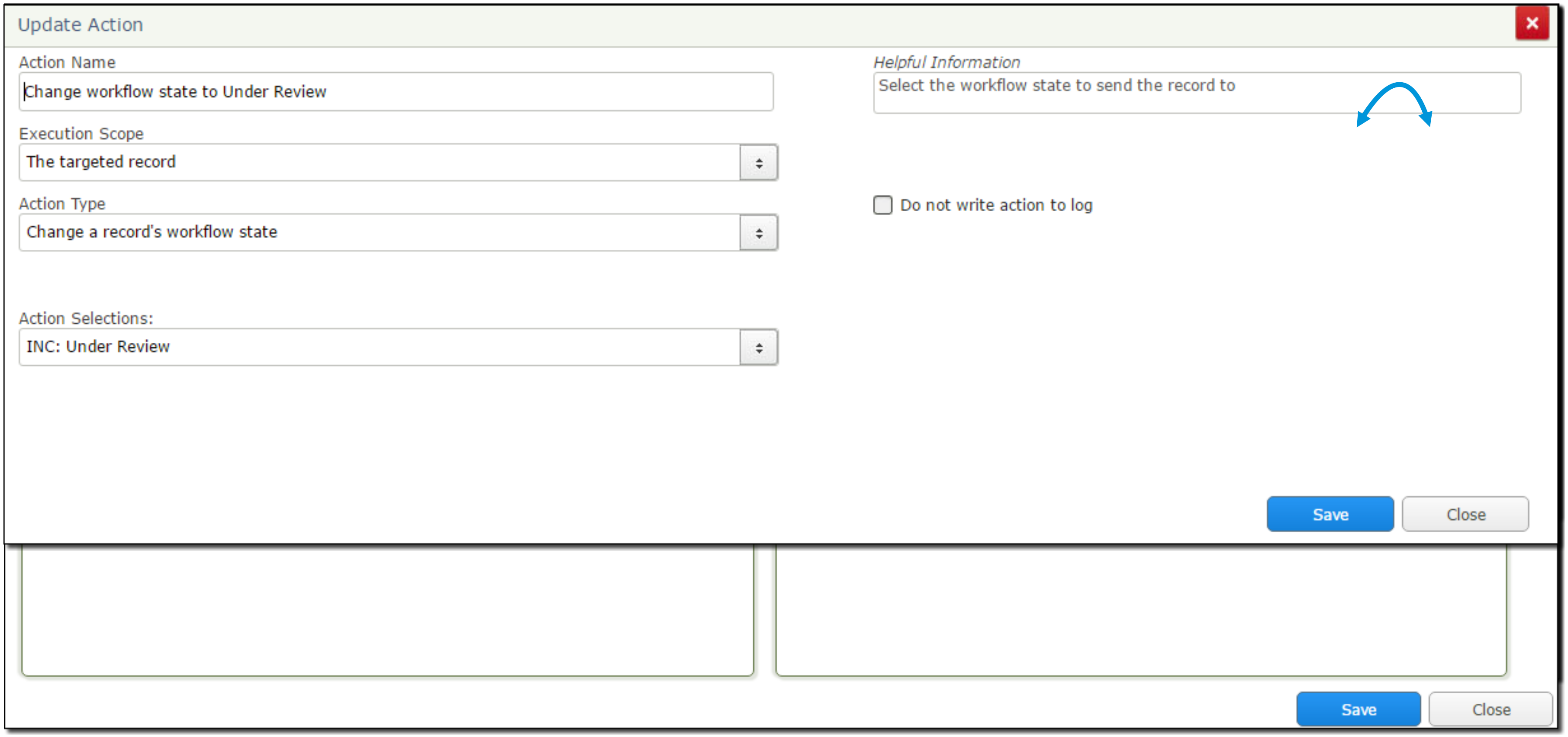
Handlers

Handlers consist of the following elements:

- Criteria: Individual checks that are performed. There may be many criteria within each handler. All criteria must pass before the handler's actions are executed
- Action: Individual actions that will be performed should all criteria within the handler pass



Managing Handlers



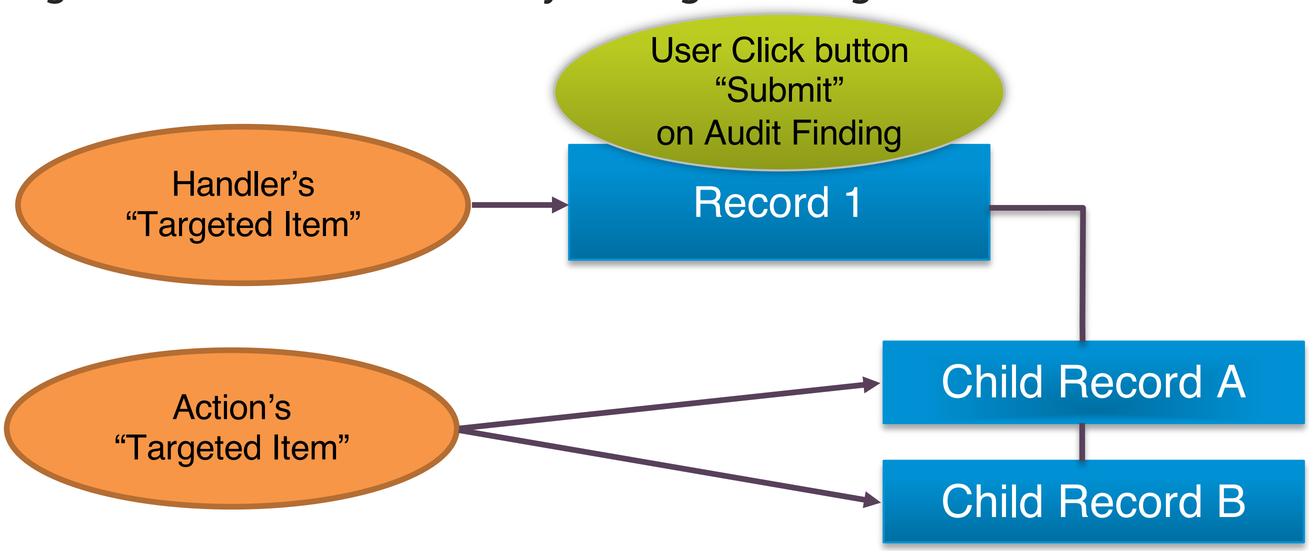
Using “On Failure” for Criteria

The following are important options to explore when deciding how to handle the failure of a Handler’s Criteria:

- **Stop Handler for the Current Item:** The default is to stop the immediate handler for the immediate record/object… which means any other handlers associated with that workflow button / event will still execute on the current record/object.
- **Stop Handler for all Items:** In the case where a handler’s execution scope is for children / parent, this option will stop the handler at the first object / record that fails and not execute the handler on other targets.
- **Stop All Handlers for this Event:** With this setting, Rsam will stop All handlers executed from the event on all items. This is popular to use because it also provides the special option to display a message to the user explaining why the handlers are stopping.

Scope

- Handlers, Actions, and Criteria have selectable Scope
- Scope determines where the Handler, Action and Criteria are executed relative to the target
  - Scope is always relative to the "Targeted Item"
  - The targeted item reference may change through the event

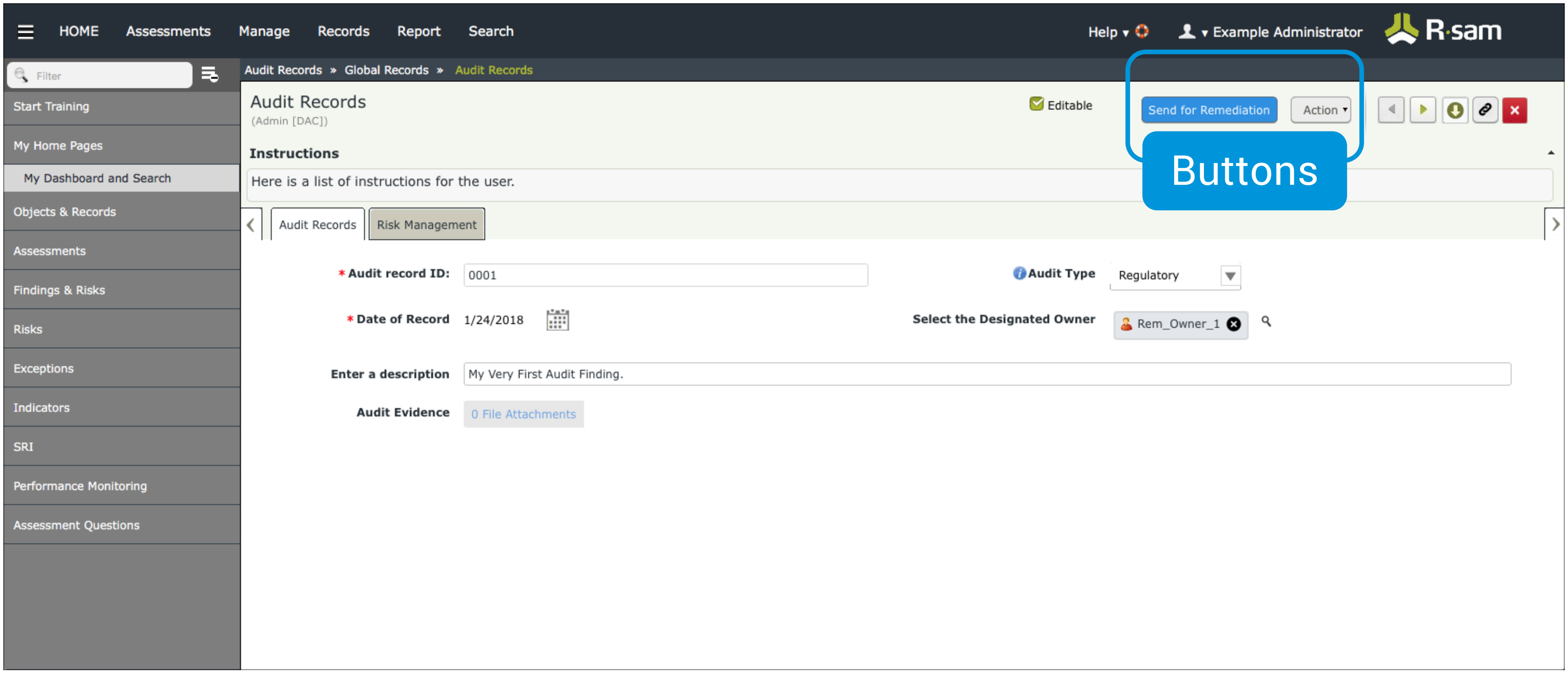


Simulated Button Clicks

- Many features in Rsam allow you to “Simulate Button Clicks”
- This allows you to create a button with Handlers, and then have Rsam pretend that a user clicked that Button
- Examples:
  - When you want to have Handlers execute when you create an Object or Record
  - When you want to have Handlers execute as part of the Import Process

What are we going to build?

Galvanize




Galvanize
Creating Workflow States, Buttons and Risk Handlers
Exercise

Galvanize

Import

Learning Objectives

Galvanize

- At Completion of this Section you will:
  - Understand what can be imported
  - Identify import sources
  - Identify the components/steps in using the import features

Data Import

Data Import allows customers to import object inventories, questionnaire responses, records, and control libraries into Rsam

- Rsam can import from the following sources:
  - Delimited text files (tab, comma, etc)
  - Excel Spreadsheets
  - XML files
  - Rsam Offline Data Gathering File
  - Database connection strings & queries
  - Third Party APIs
  - Email messages

- During import Rsam can:
  - Add new objects, records, control types
  - Update existing objects and records
  - Trigger Workflow Buttons and Event Handlers

Imports can be performed manually, scheduled for automation, or triggered via an event handler

General Import Process

When importing data into Rsam, you will need to perform some or all of the following steps:

- Import Page: Select a data source, or saved profiled from a prior import
- General Tab: Specify where the data will be placed in Rsam (object, object type, entity, record category, etc.)
- Mapping Tab: Map values from your data source into fields in Rsam (such as attributes, controls, criticality)
- Filter Tab: Specify any filters you wish to apply to the data before importing
- Action Tab: Tell Rsam how you would like to handle:
  - The creation of new Objects / Records
  - The update of existing Objects / Records
  - Detection of previously imported Objects / Records that are absent
- Unique ID: Specify which fields will be used to identify existing records /objects
- Definition: Special use-case for handling separated library elements inside of the imported file
- Translation: Specify any character or word substitutions that should occur during import (e.g. translating “3” to “High Risk”)
- Management: Save your mapping & profile settings, test the import, and perform the actual import itself

Importing Data into Rsam (Records Based)

Exercise

Galvanize

Searches and Charts

Learning Objectives

- At Completion of this Section you will:
  - Understand the purpose of Searches and Charts
  - Understand how to create searches and charts
  - Understand and identify where searches and charts can be used

Uses for Searches

Searches allow customers to perform a basic or advanced search through Objects, Records, Logs and Performance data

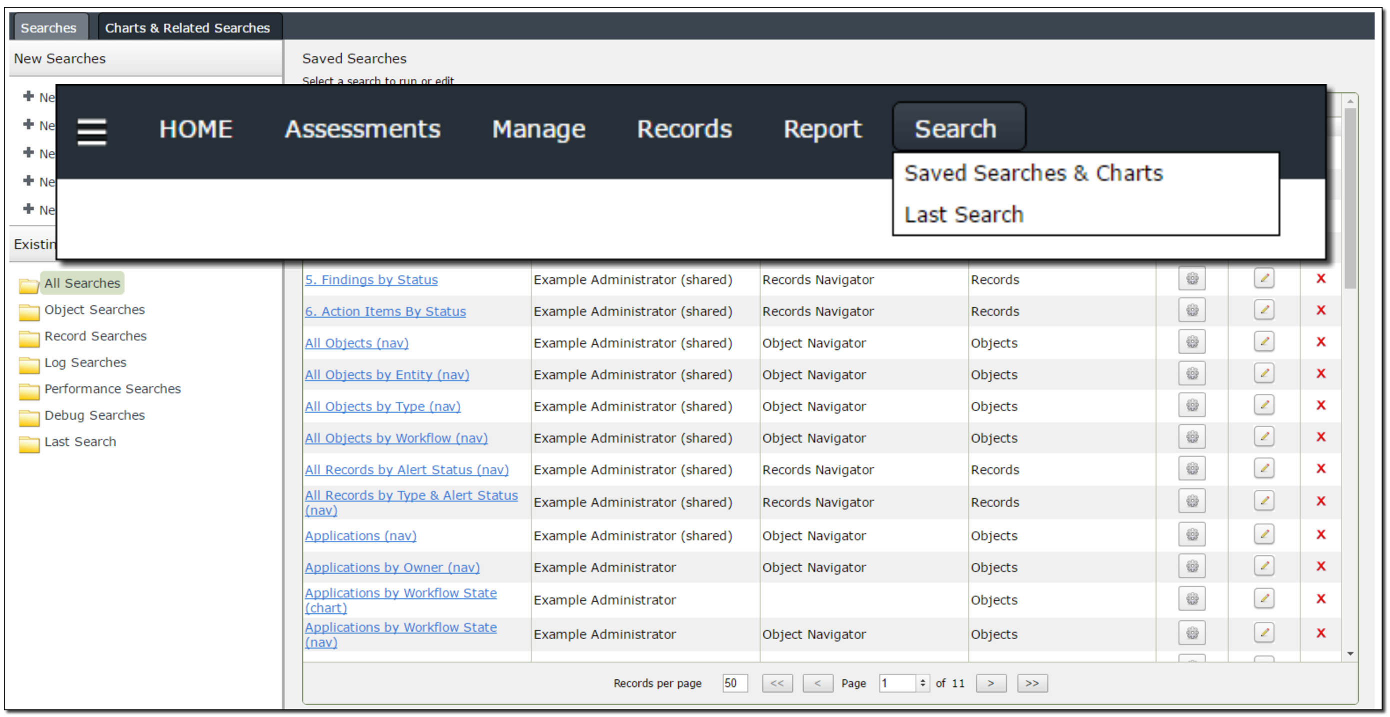
- Searches can be saved for later use
- Saved Searches can be used to:
  - Share with other users via their roles
  - Have their results shown on the home page
  - Generate Charts & Dashboards
  - As a navigation tree in the Objects & Records Navigator
  - Provide dynamic response sets for Attributes
  - Create custom SSRS reports
- When someone asks for a report, start by building a search
  - 80%* of report requests are fulfilled by simply making a search
  - Most of the remaining are reports built off of search results

* Highly Scientific poll, completed by Gallup, CNN, Nielsen and audited by PwC. Not to be confused by a random number plucked from the air.

Search Selection

Access the Search Navigator through the Rsam Menu

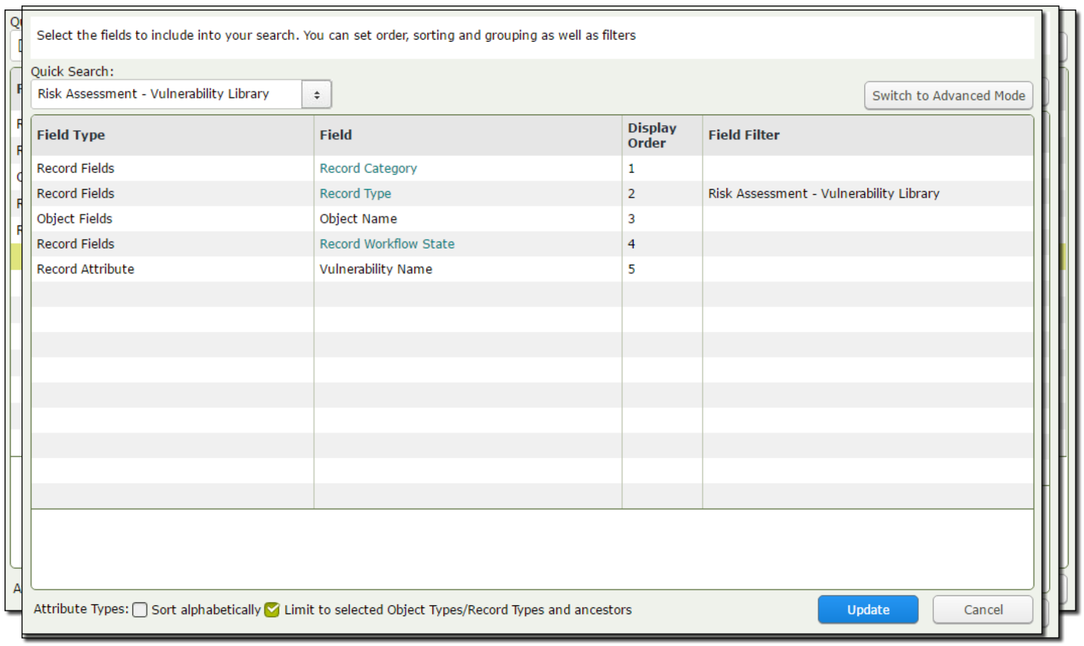
- One-click access to existing searches, options, criteria & new searches



Search Criteria

Search results are driven off of Search Criteria

- Search Criteria allow you to specify the fields to display, field order, filters, sort order, display options, groupings, summary aggregation & more



Search Results

Searches pull live data from Rsam and allow you to:

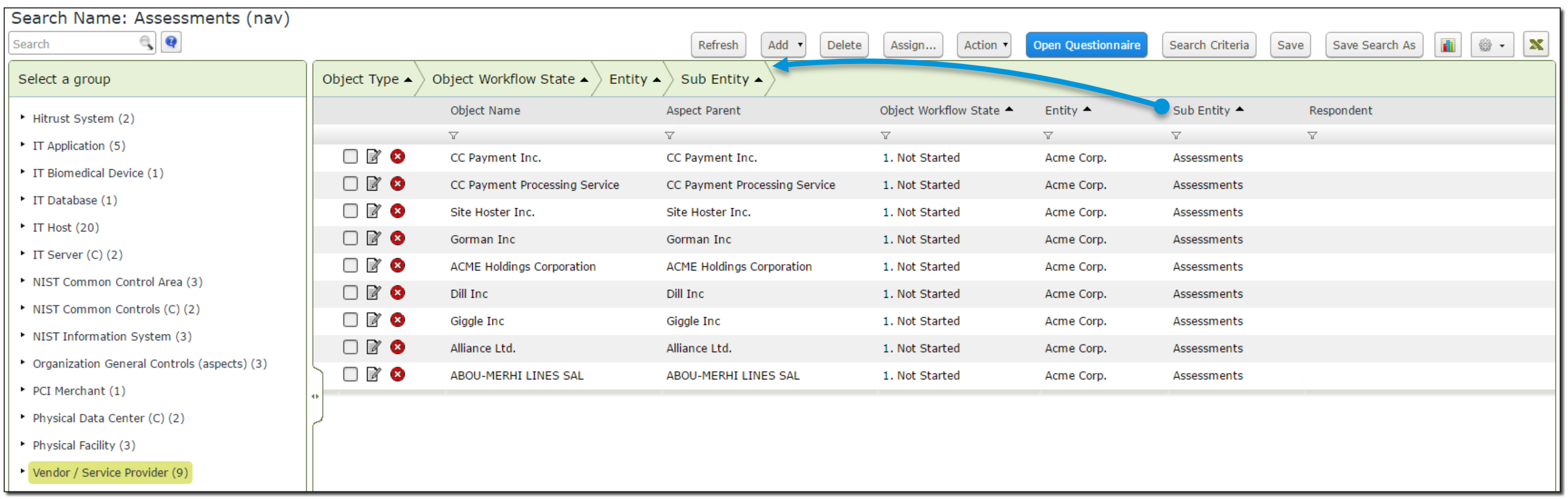
- View search results
- Dynamically drag & drop columns to perform groupings
- Navigate to a search result, or open the result directly
- Perform Workflow actions across many Records / Objects at once
- Perform mass edits
- Export the results to various file formats
- Save the Search Criteria for future uses

Grouping Search Results

Galvanize

Search results can be grouped for better navigation and to build charts and navigators:

- Build one or more groups by dragging column headers into the section above the search results
- Groupings are generated on the left side, allowing for quick and easy navigation



Charting Search Results

Search results can be used to create charts:

- Charts can be generated using the search groupings and pivot points
- Charts reflect the search filters, groupings, and aggregation selections
- Charts are rendered on-the-fly, making it easy to preview chart properties and groupings
- Charts can be saved for later use, and even published to home pages

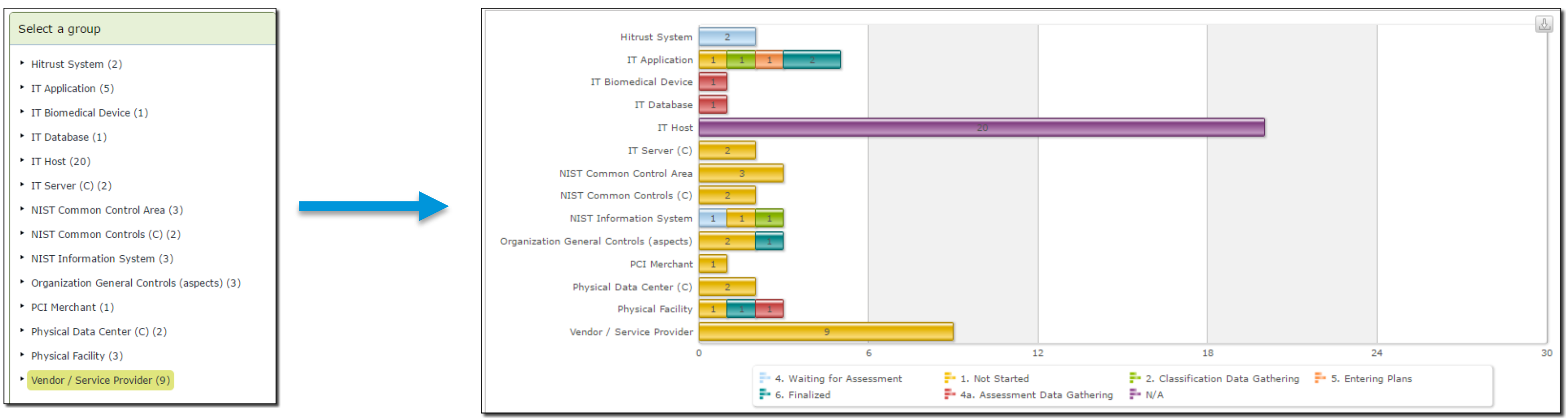
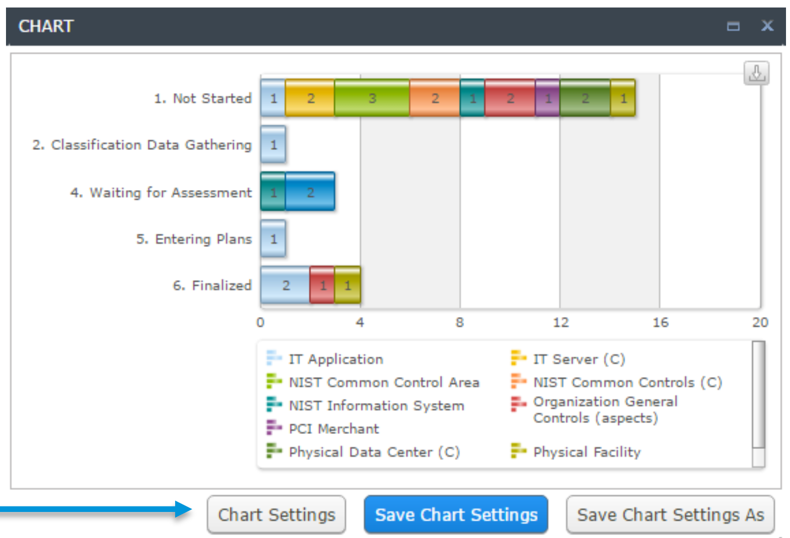


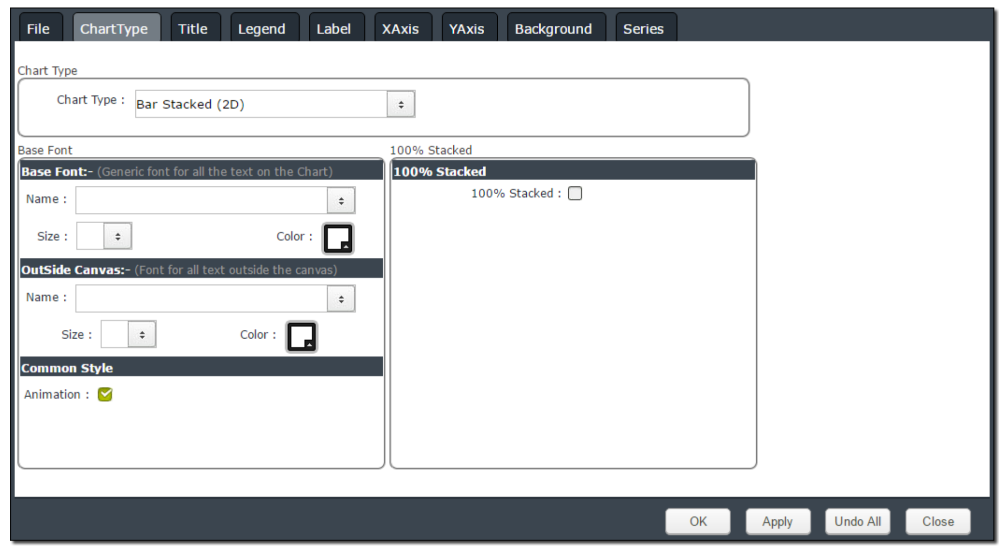
Chart Settings

Galvanize

Charts have extensive options:

- Using the Chart Settings button, you can select new chart types, and many different chart properties

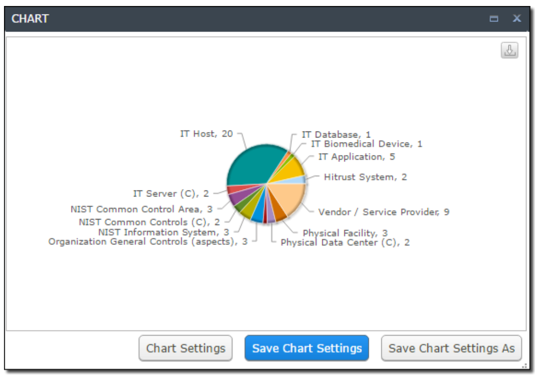


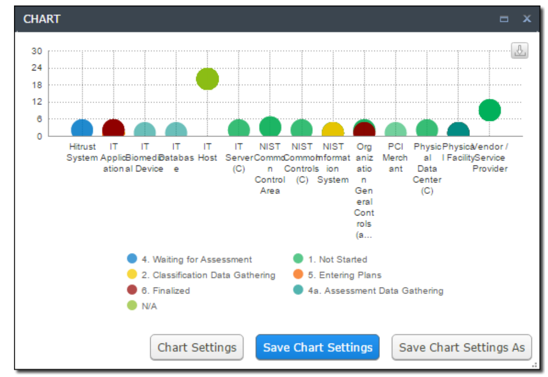


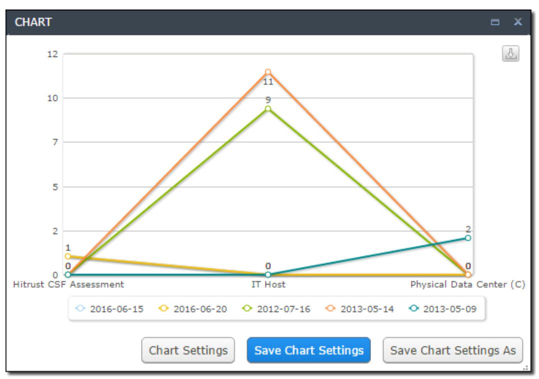
- Charts can also be saved for future use, or to publish in a home page tab

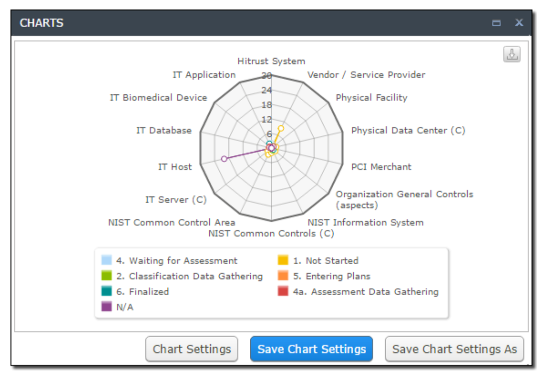
Example Charts

A few examples of available charting options





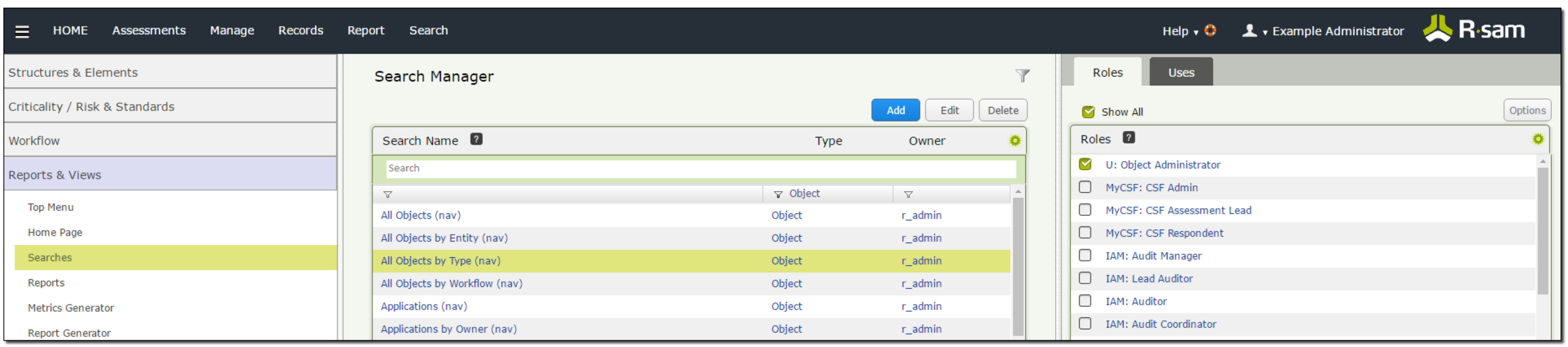




Search Manager

Administrators have access to all saved searches & can:

- Add / Modify / Delete Saved Searches
- Assign Saved Searches to roles, granting access to:
  - Execute a search
  - Edit the actual search options



Galvanize

Home Screens & Home Page Designer

Learning Objectives

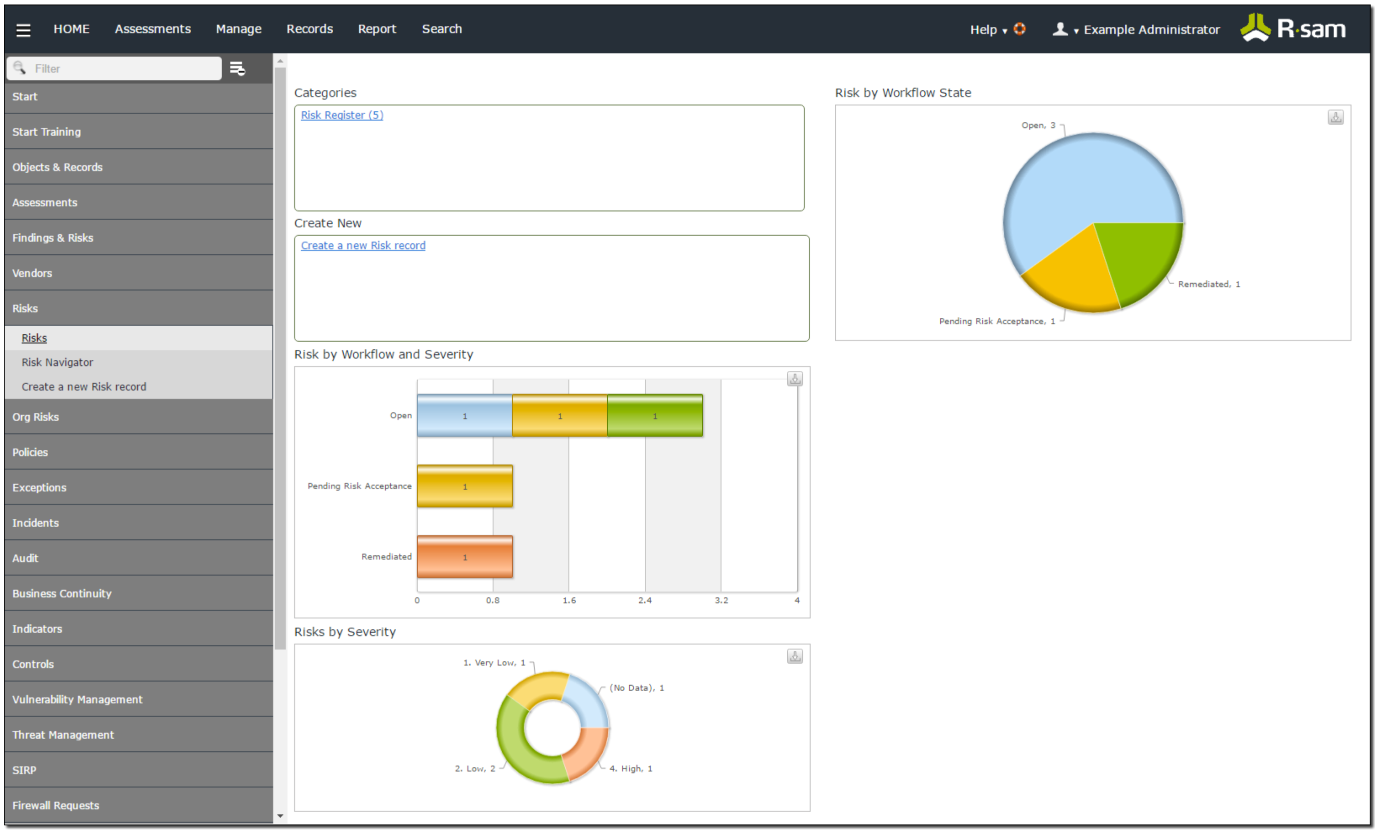
- At Completion of this Section you will:
  - Understand the purpose of Home Pages
  - Understand Home Page Design Options
  - Understand Activity Centers
  - Understand the use of different types of tabs
  - Understand the use of inline editing

Home Screen Tabs

Home Page Tabs are the primary method used by users to navigate through Rsam, from the landing page across to access all of their accessible modules

- Rsam includes OOTB home page tabs with each module, but customers often create their own allowing for customized views of data, and navigation
- Each home page tab can contain one or more widgets/activity centers. Widgets & Acticity Centers can display lists of information, charts / dashboards, shortcuts to functional areas, and more.
- Home screen tabs are associated with roles; therefore, different users will have access to specific tabs based on their role assignments

Home Page Widgets/Activity Centers



Home Page Design

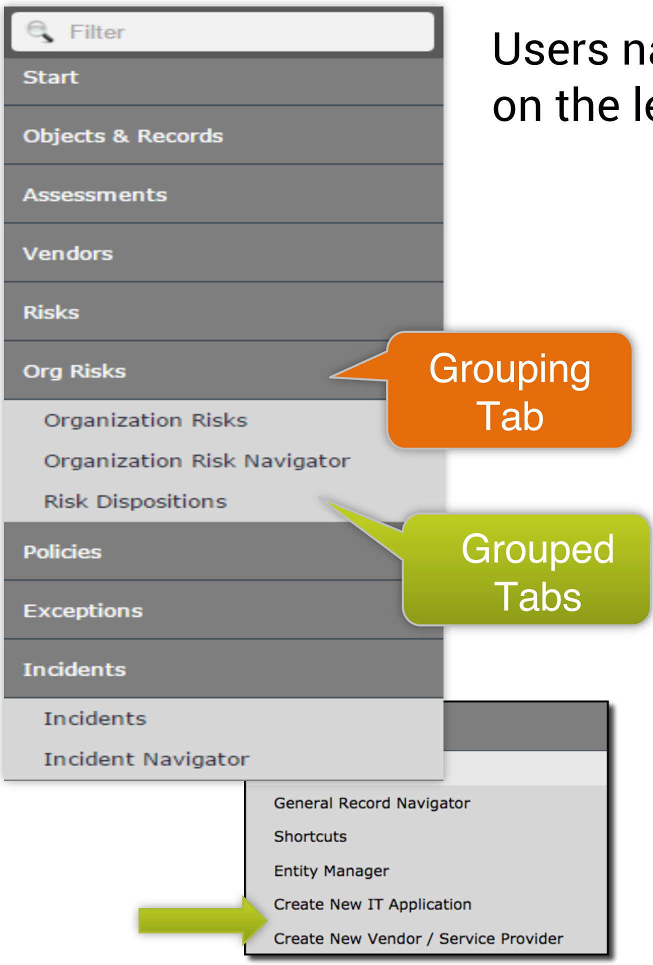
- This new features is only available with v10
- No longer limited to 2 column layout (Technically limited to 16)
- Simple widget drag and drop & resizing capability
- Administrators can now modify home page tabs directly on the page not just via the admin screen.
  - Currently, new pages must still be created via the admin screen though
- Widgets can be set to collapse/load on-demand speeding up page loads
- Widgets now support Role Based Access

Activity Centers

- This new features is only available with v10
- Simpler, centralized access to activities across all modules
- Create multiple activity centers in standard pages & object navigators
- Numeric and color indicators can be set to highlight the importance of the center
- Activity Centers support Role Based Access

Left Navigation Panel

Galvanize



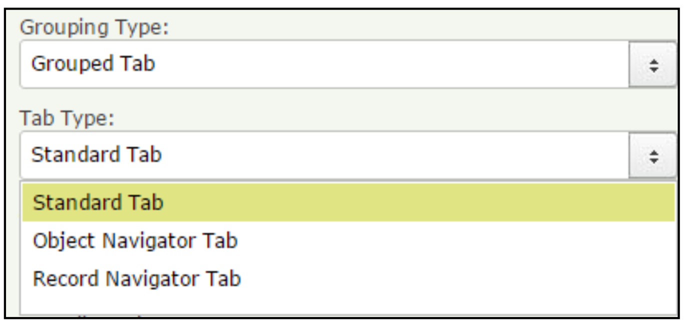
Users navigate to their home pages using a navigation panel located on the left side of the screen

- Tabs are divided into Grouping Tabs and Grouped Tabs
  - Grouping Tabs: contain one or more Grouped Tabs
  - Grouped Tabs: contain the widgets/activity centes
- Stand-Alone tabs are also available, and they appear as both a Grouping & Grouped tab
- Tabs are searchable / filterable by the end user
- Self Registration Links for Records and Object can also appear in grouping tabs for quick access
- Leverage Grouping / Grouped tabs (no need to use stand-alone tabs)
- Use consistent wording in Home Page Tabs (like “Dashboard”)

Types of Tabs

Group Tabs and Stand-Alone Tabs are classified into the following Tab Types

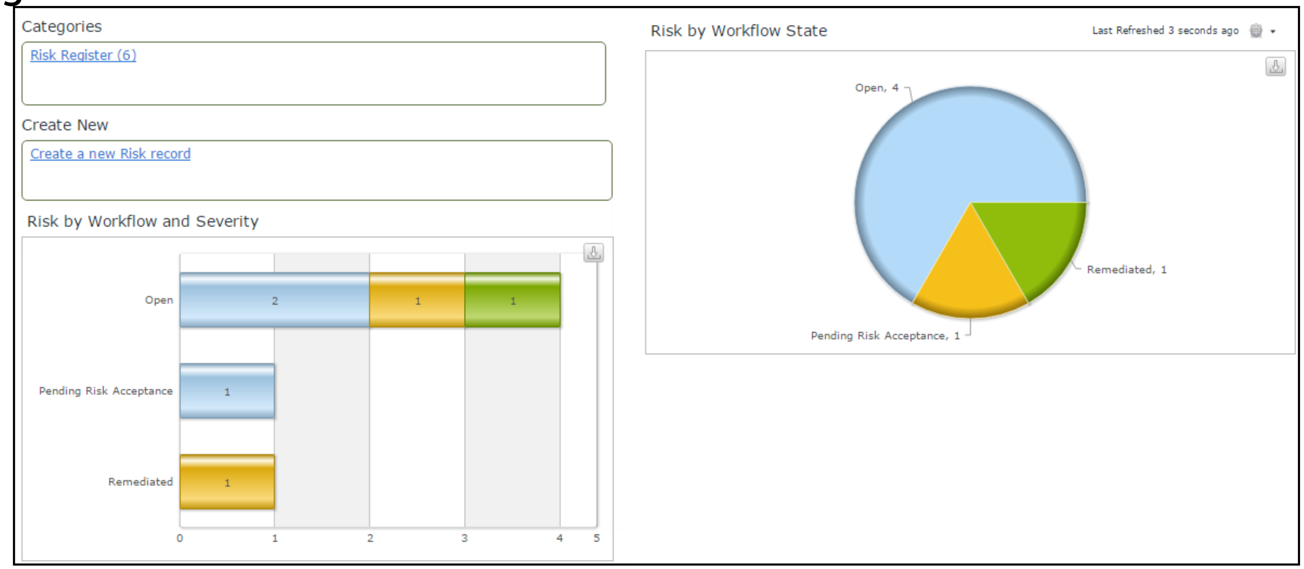
- Standard Tabs
- Record Navigator Tabs
- Object Navigator Tabs



Standard Tabs

This is the most common type of Tab used by customers

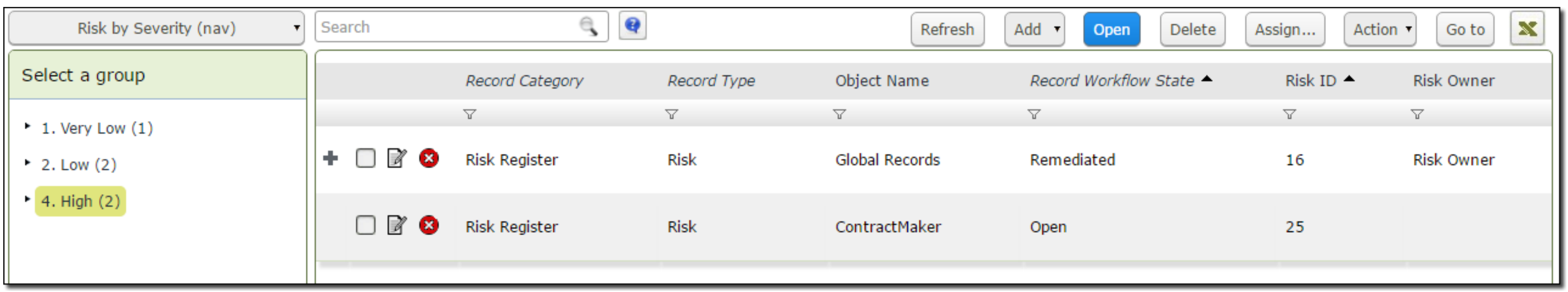
- Basic tabs which holds multiple widgets… often providing access to different parts of the application (links to searches, dashboards, cosmetics, and more)
- Often used for a home page for a specific module, dashboards, and other pages that require multiple widgets



Record Navigator Tabs

Tabs dedicated to showing lists of records using a variety of filters and groupings

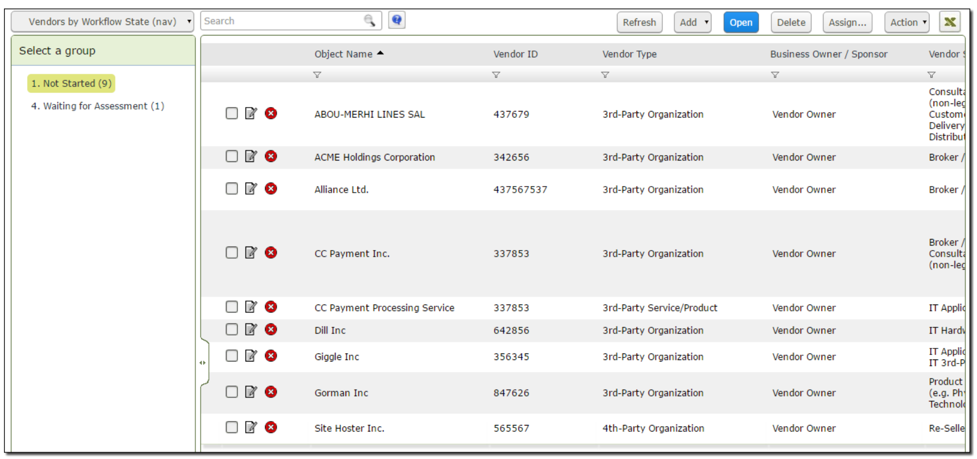
- Often used as searchable task queues and for records that need quick and simple access for users
- Leverages Record Searches to present the lists of records

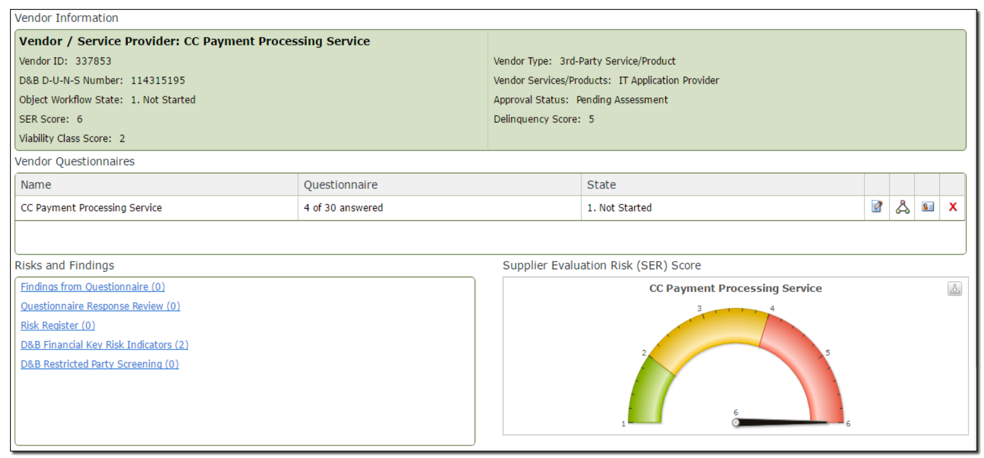


Object Navigator Tabs

Dedicated to showing lists of objects, and then allowing the user to drill into the object to gain access to the various object components

- This is a more advanced tab, often used to provide a holistic view of an object
- This type of tab leverages Object Searches to present the lists of objects, and then individual widgets to show the details once inside of an object

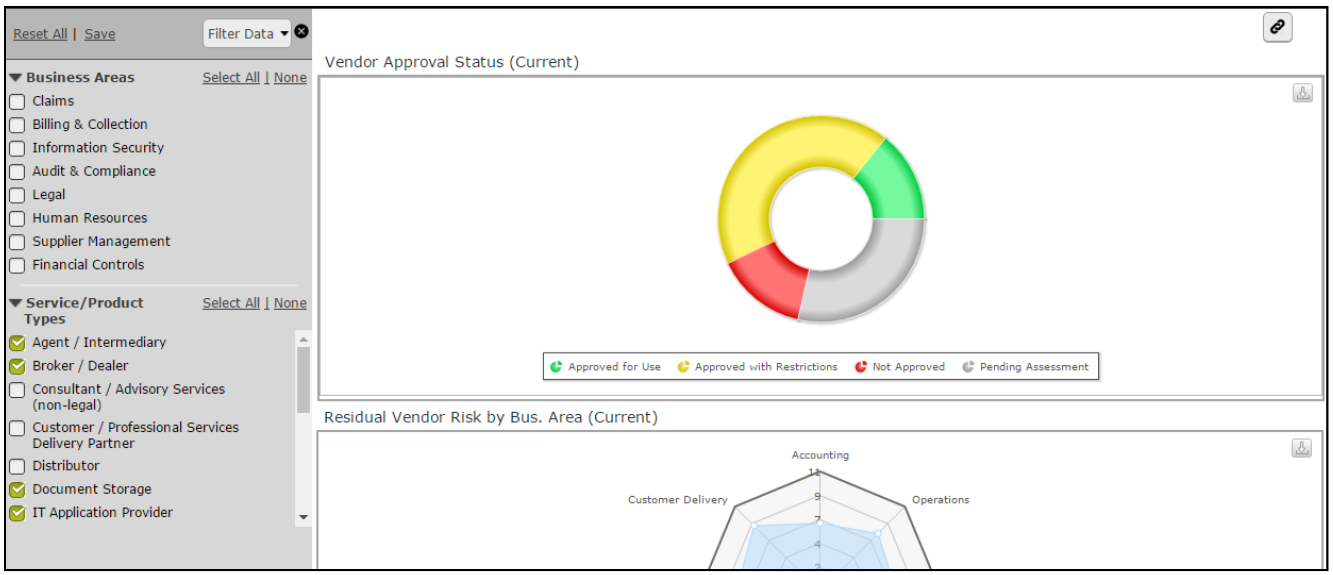




Tab Filters

Standard Tabs support a special feature called “Dynamic Filters”

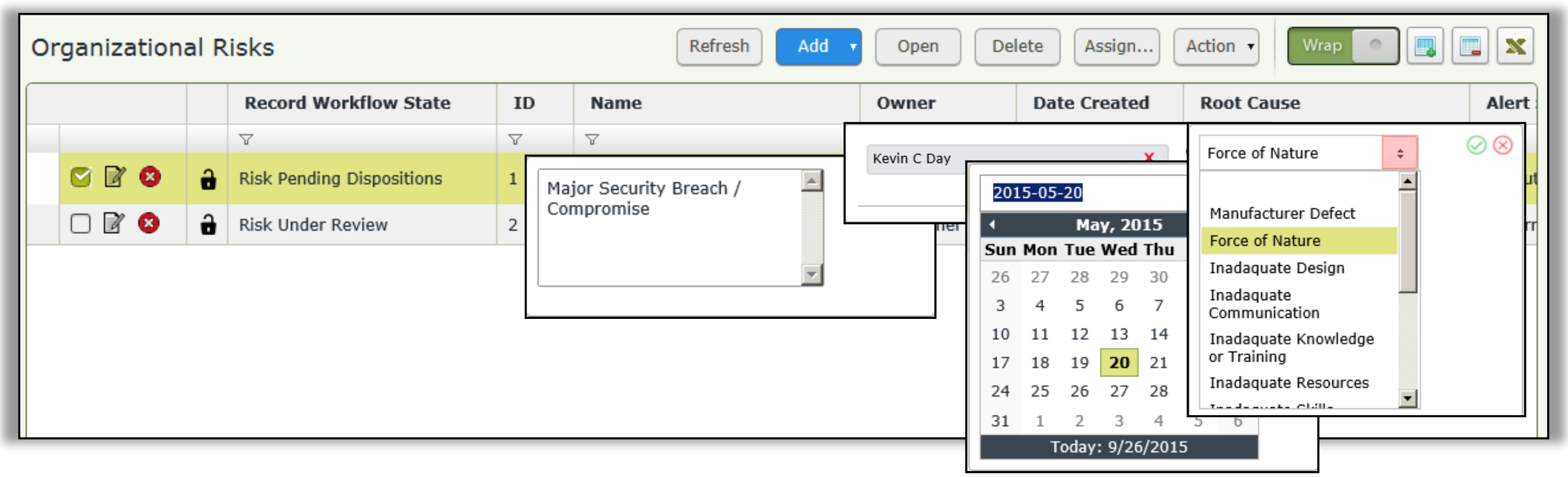
- Administrators can place special filter selections on the left side of the screen
- Users can interact with these selections to filter the content that is being presented on the right



Inline Editing

Record and Object Attributes can be edited directly from a list, search, or navigator

- Quick way to edit without having to load the record/object form
- Functions in child grids as well
- Works with on-screen handlers and other events



Inline Editing

- Create searches and navigators to expose commonly edited attributes to users
- Record types have an option to “simulate workflow button click” when completing an inline edit. Take advantage of this to execute handlers based on inline edit results
- Note that each individual row / cell commits to the DB at the completion of that inline edit
- There is no multi-select inline editing… if you want to edit multiple records, you need to multi-select and “open”

Galvanize

Creating and Configuring Searches, Charts & Home Pages

Exercise

Galvanize

Reporting

Learning Objectives

- At Completion of this Section you will:
  - Understand the different reporting options available to you

Reporting Engine

- Rsam includes many methods of reporting, each satisfies a different need
  - The reporting needs across Rsam customers varies greatly. So Rsam focuses on providing many reporting opportunities
  - Some of these reporting methods are used by all customers, while others are only used by a small subset of customers

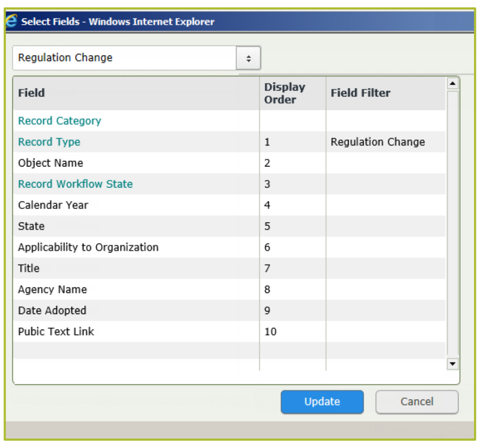
Reporting Opportunities in Rsam

- The following reporting methods are available with Rsam

Report / Dashboard Interface	Who can create	Difficulty	Effort	Data Flexibility	Presentation Flexibility	Launched from Rsam
Rsam - Search & Pivot	Anyone in Rsam	Low	Low	High	Low	Yes
Rsam - Drag & Drop Charting	Anyone in Rsam	Low	Low	High	Medium	Yes
Rsam - Default Report Templates	N/A	N/A	Low	Low	Very Low	Yes
Rsam - Rapid Reports	Anyone (assigned by Role)	Medium	Low	Medium	Medium	Yes
Custom - Report / Dashboard Via Rsam SSRS	Knowledge of SSRS Interface	Medium	Low	High	Very High	Yes
Custom - Report / Dashboard Via custom SSRS	Knowledge of SQL and SSRS Interface	High	Medium	Very High	Very High	Yes
Custom - Report / Dashboard Via Crystal Reports	Knowledge of SQL & Crystal Interface	High	High	Very High	Very High	Yes
Custom - Report / Dashboard Via external package (Cognos, Bo, Home Grown, Etc)	Knowledge of SQL & External Tool	High	High	Very High	Very High	No

Searches and Pivots

- Searches are the primary reporting mechanism.
  - Tell Rsam what you want to see
  - How you want it filtered, sorted, and grouped.
- Rsam will show you the information, allowing you to show details, execute actions, or export the results.

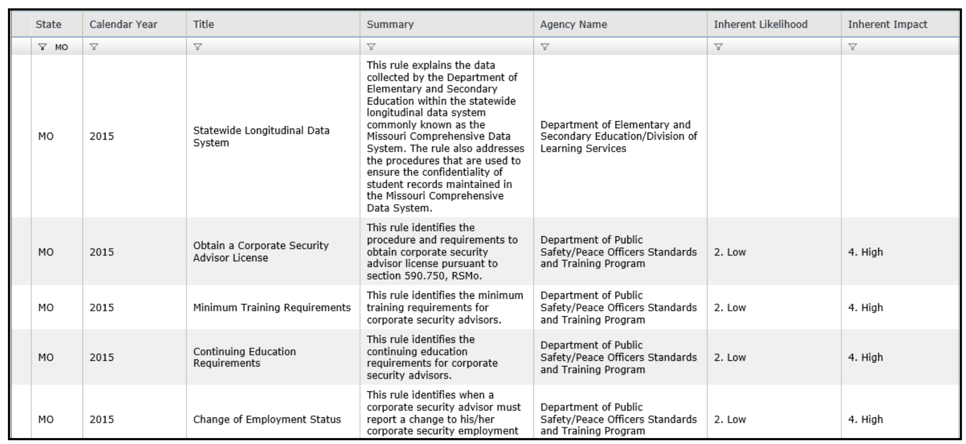


Select Fields - Windows Internet Explorer

Regulation Change

Field	Display Order	Field Filter
Record Category		
Record Type	1	Regulation Change
Object Name	2	
Record Workflow State	3	
Calendar Year	4	
State	5	
Applicability to Organization	6	
Title	7	
Agency Name	8	
Date Adopted	9	
Pubic Text Link	10	

Update Cancel



State	Calendar Year	Title	Summary	Agency Name	Inherent Likelihood	Inherent Impact
MO						
MO	2015	Statewide Longitudinal Data System	This rule explains the data collected by the Department of Elementary and Secondary Education within the statewide longitudinal data system commonly known as the Missouri Comprehensive Data System. The rule also addresses the procedures that are used to ensure the confidentiality of student records maintained in the Missouri Comprehensive Data System.	Department of Elementary and Secondary Education/Division of Learning Services		
MO	2015	Obtain a Corporate Security Advisor License	This rule identifies the procedure and requirements to obtain corporate security advisor license pursuant to section 590.750, RSMo.	Department of Public Safety/Peace Officers Standards and Training Program	2. Low	4. High
MO	2015	Minimum Training Requirements	This rule identifies the minimum training requirements for corporate security advisors.	Department of Public Safety/Peace Officers Standards and Training Program	2. Low	4. High
MO	2015	Continuing Education Requirements	This rule identifies the continuing education requirements for corporate security advisors.	Department of Public Safety/Peace Officers Standards and Training Program	2. Low	4. High
MO	2015	Change of Employment Status	This rule identifies when a corporate security advisor must report a change to his/her corporate security employment	Department of Public Safety/Peace Officers Standards and Training Program	2. Low	4. High

Reporting Opportunities in Rsam

- The following reporting methods are available with Rsam

Report / Dashboard Interface	Who can create	Difficulty	Effort	Data Flexibility	Presentation Flexibility	Launched from Rsam
Rsam - Search & Pivot	Anyone in Rsam	Low	Low	High	Low	Yes
Rsam - Drag & Drop Charting	Anyone in Rsam	Low	Low	High	Medium	Yes
Rsam - Default Report Templates	N/A	N/A	Low	Low	Very Low	Yes
Rsam - Rapid Reports	Anyone (assigned by Role)	Medium	Low	Medium	Medium	Yes
Custom - Report / Dashboard Via Rsam SSRS	Knowledge of SSRS Interface	Medium	Low	High	Very High	Yes
Custom - Report / Dashboard Via custom SSRS	Knowledge of SQL and SSRS Interface	High	Medium	Very High	Very High	Yes
Custom - Report / Dashboard Via Crystal Reports	Knowledge of SQL & Crystal Interface	High	High	Very High	Very High	Yes
Custom - Report / Dashboard Via external package (Cognos, Bo, Home Grown, Etc)	Knowledge of SQL & External Tool	High	High	Very High	Very High	No

Drag and Drop Charting

Grouped searches can quickly transform into informative charts & dashboards

Reporting Opportunities in Rsam

Galvanize

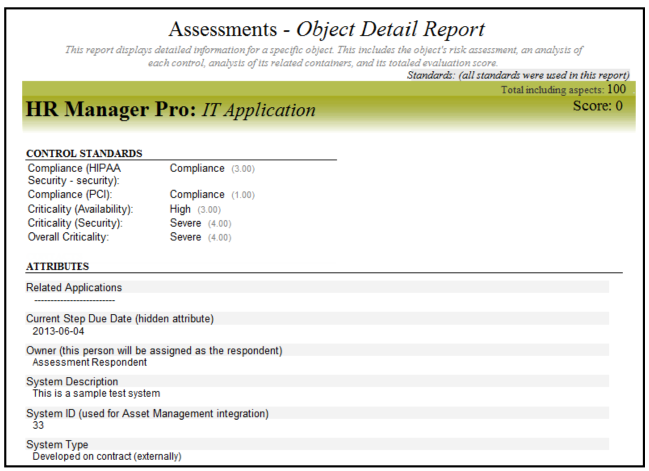
- The following reporting methods are available with Rsam

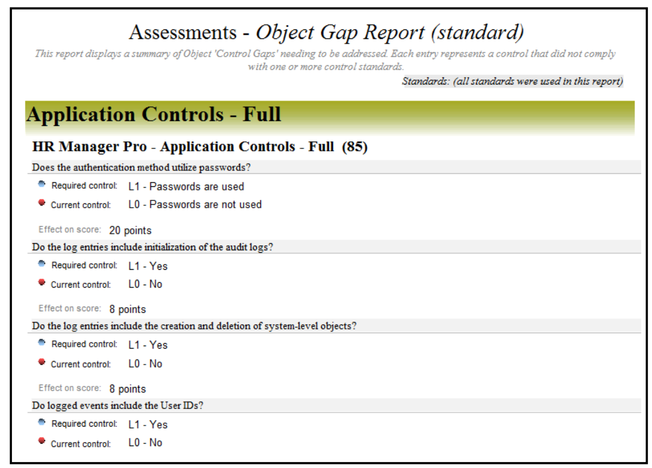
Report / Dashboard Interface	Who can create	Difficulty	Effort	Data Flexibility	Presentation Flexibility	Launched from Rsam
Rsam - Search & Pivot	Anyone in Rsam	Low	Low	High	Low	Yes
Rsam - Drag & Drop Charting	Anyone in Rsam	Low	Low	High	Medium	Yes
Rsam - Default Report Templates	N/A	N/A	Low	Low	Very Low	Yes
Rsam - Rapid Reports	Anyone (assigned by Role)	Medium	Low	Medium	Medium	Yes
Custom - Report / Dashboard Via Rsam SSRS	Knowledge of SSRS Interface	Medium	Low	High	Very High	Yes
Custom - Report / Dashboard Via custom SSRS	Knowledge of SQL and SSRS Interface	High	Medium	Very High	Very High	Yes
Custom - Report / Dashboard Via Crystal Reports	Knowledge of SQL & Crystal Interface	High	High	Very High	Very High	Yes
Custom - Report / Dashboard Via external package (Cognos, Bo, Home Grown, Etc)	Knowledge of SQL & External Tool	High	High	Very High	Very High	No

Templated Reports

Rsam includes a series of templated reports that show details and summaries of object data

- While these reports are static they can be helpful in showing a quick view of an object, or aggregation of control / domain compliance
- These reports focus on the object / questionnaire information





Reporting Opportunities in Rsam

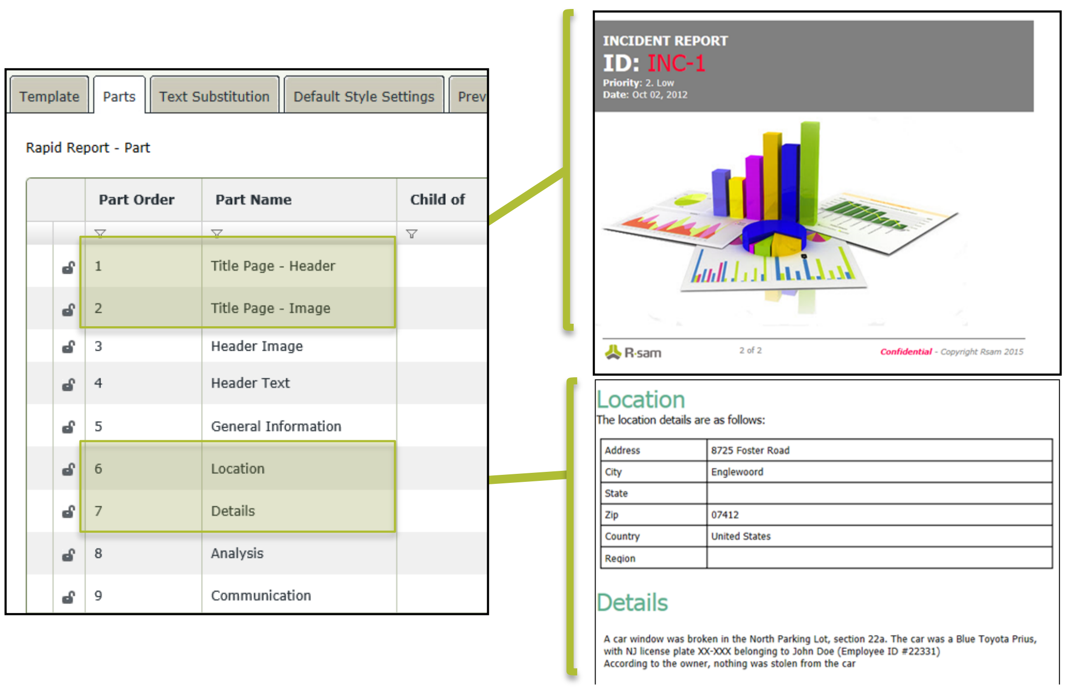
Galvanize

- The following reporting methods are available with Rsam

Report / Dashboard Interface	Who can create	Difficulty	Effort	Data Flexibility	Presentation Flexibility	Launched from Rsam
Rsam - Search & Pivot	Anyone in Rsam	Low	Low	High	Low	Yes
Rsam - Drag & Drop Charting	Anyone in Rsam	Low	Low	High	Medium	Yes
Rsam - Default Report Templates	N/A	N/A	Low	Low	Very Low	Yes
Rsam - Rapid Reports	Anyone (assigned by Role)	Medium	Low	Medium	Medium	Yes
Custom - Report / Dashboard Via Rsam SSRS	Knowledge of SSRS Interface	Medium	Low	High	Very High	Yes
Custom - Report / Dashboard Via custom SSRS	Knowledge of SQL and SSRS Interface	High	Medium	Very High	Very High	Yes
Custom - Report / Dashboard Via Crystal Reports	Knowledge of SQL & Crystal Interface	High	High	Very High	Very High	Yes
Custom - Report / Dashboard Via external package (Cognos, Bo, Home Grown, Etc)	Knowledge of SQL & External Tool	High	High	Very High	Very High	No

Rapid Reports

- Rapid Reports is a powerful and flexible way to create “documentation style” reports
- Rapid Report templates are created and managed under the:
  - Records Menu: Rapid Report Templates



Reporting Opportunities in Rsam

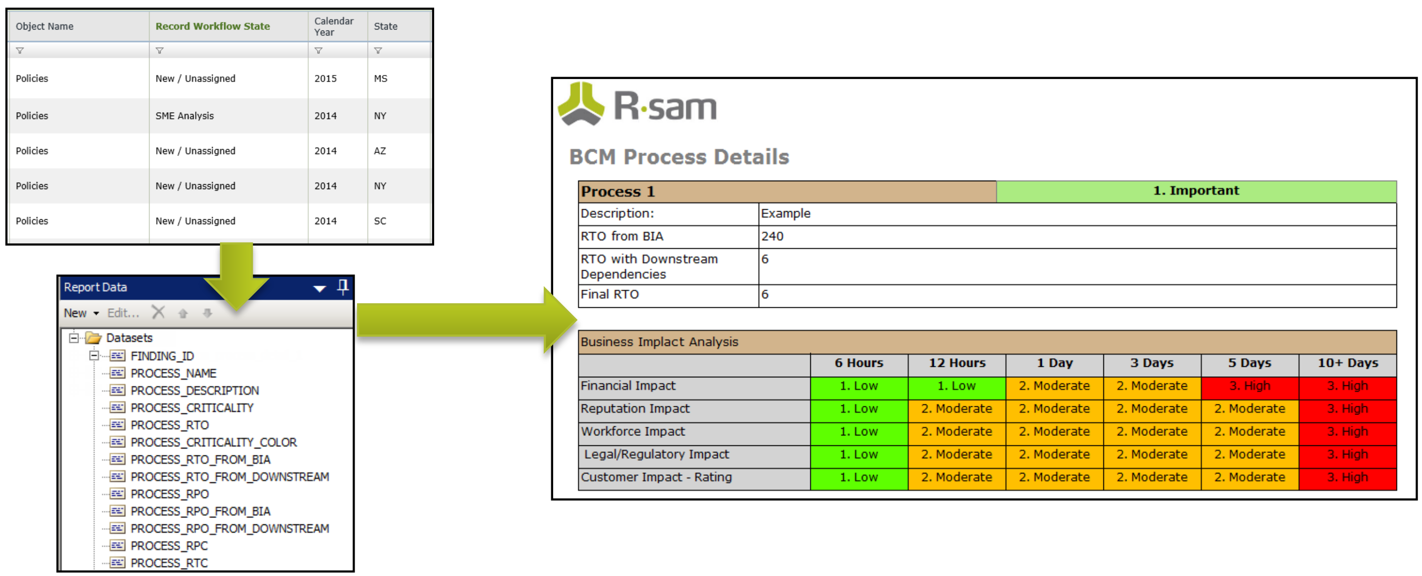
- The following reporting methods are available with Rsam

Report / Dashboard Interface	Who can create	Difficulty	Effort	Data Flexibility	Presentation Flexibility	Launched from Rsam
Rsam - Search & Pivot	Anyone in Rsam	Low	Low	High	Low	Yes
Rsam - Drag & Drop Charting	Anyone in Rsam	Low	Low	High	Medium	Yes
Rsam - Default Report Templates	N/A	N/A	Low	Low	Very Low	Yes
Rsam - Rapid Reports	Anyone (assigned by Role)	Medium	Low	Medium	Medium	Yes
Custom - Report / Dashboard Via Rsam SSRS	Knowledge of SSRS Interface	Medium	Low	High	Very High	Yes
Custom - Report / Dashboard Via custom SSRS	Knowledge of SQL and SSRS Interface	High	Medium	Very High	Very High	Yes
Custom - Report / Dashboard Via Crystal Reports	Knowledge of SQL & Crystal Interface	High	High	Very High	Very High	Yes
Custom - Report / Dashboard Via external package (Cognos, Bo, Home Grown, Etc)	Knowledge of SQL & External Tool	High	High	Very High	Very High	No

Rsam Generated SSRS Reports via Search

Galvanize

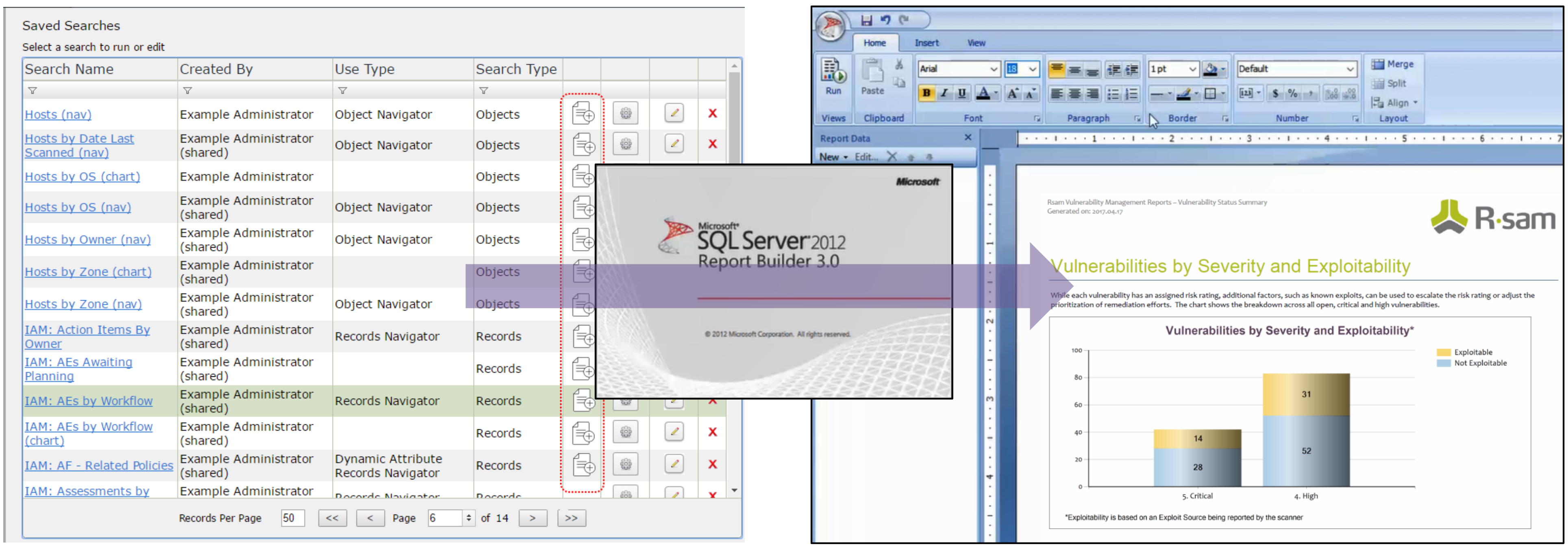
- SSRS reports via Rsam Searches transform search results into fully customizable reports. The most flexible method for reporting without the need to understand the database
- Requires the report writer to use Microsoft Visual Studio to author and manage the report



Using the new Report Builder

Galvanize

- Users can build / edit reports without having to install Visual Studio
- Access directly from the search and reporting screens
- Can work in customer environments and Rsam Cloud



Using the new Report Builder

- This new method, while far better than before, carries important limitations:
  - Server configuration to enable this feature requires 30-60 minutes to setup.
  - Contact support for help when doing this.

- Like before, the permission model is centralized. In the cloud (and most on-prem customers), those users who are given access to build and publish reports have full access to query Rsam & see other reports.
  - Consider these individual to be report admins (access to all data).

- For most customers (SQL 2014 and earlier), the report builder will only launch using Internet Explorer (though the resulting report can work in standard Rsam browsers).

- Despite these considerations, this new feature is well worth the effort, and is a significant improvement beyond our previous SSRS report creation process.

Reporting Opportunities in Rsam

- The following reporting methods are available with Rsam

Report / Dashboard Interface	Who can create	Difficulty	Effort	Data Flexibility	Presentation Flexibility	Launched from Rsam
Rsam - Search & Pivot	Anyone in Rsam	Low	Low	High	Low	Yes
Rsam - Drag & Drop Charting	Anyone in Rsam	Low	Low	High	Medium	Yes
Rsam - Default Report Templates	N/A	N/A	Low	Low	Very Low	Yes
Rsam - Rapid Reports	Anyone (assigned by Role)	Medium	Low	Medium	Medium	Yes
Custom - Report / Dashboard Via Rsam SSRS	Knowledge of SSRS Interface	Medium	Low	High	Very High	Yes
Custom - Report / Dashboard Via custom SSRS	Knowledge of SQL and SSRS Interface	High	Medium	Very High	Very High	Yes
Custom - Report / Dashboard Via Crystal Reports	Knowledge of SQL & Crystal Interface	High	High	Very High	Very High	Yes
Custom - Report / Dashboard Via external package (Cognos, Bo, Home Grown, Etc)	Knowledge of SQL & External Tool	High	High	Very High	Very High	No

Other Reports Via Query

- Rsam allows direct queries against the Rsam database. While this is more complex and requires far more expertise, it does allow for unrestricted custom reporting against Rsam that can be used in popular reporting platforms like:
  - SSRS
  - Crystal
  - Cognos
  - Others
- Rsam also include an API to gather data for reporting, and some helper SQL procedures to limit the amount of custom query writing

Galvanize

Structures and Elements

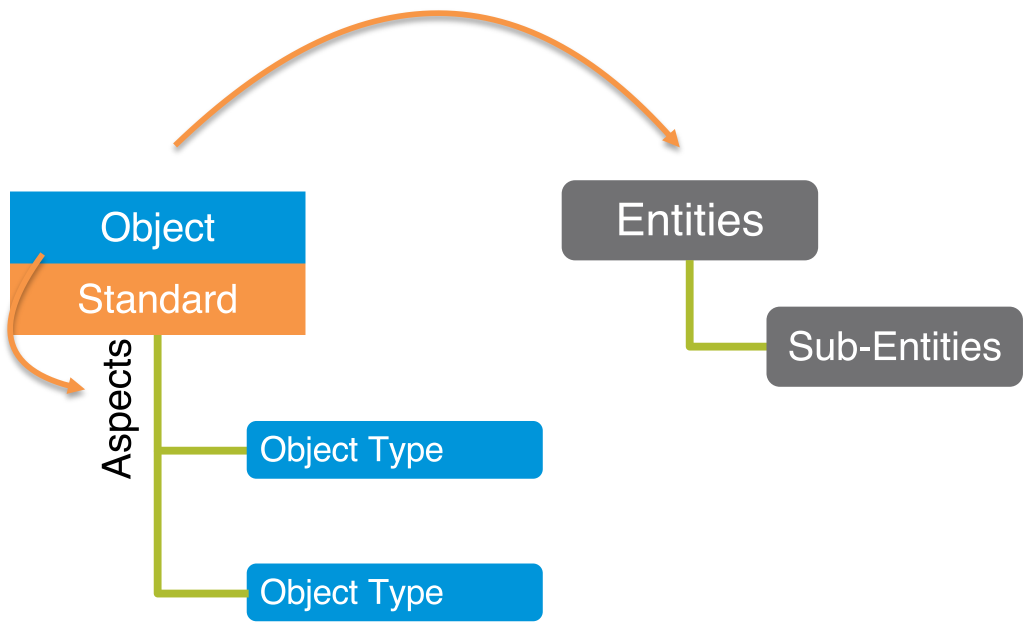
Objects

Questionnaire Basics / Learning Objectives

- Understand and identify the different types of Objects
- Understand the purpose of and how to Create / Configure Standard Object Types (Templates)
- Understand the purpose of and how to Create / Configure Criticality Types and Risk Levels
- Understand the purpose of and how to Create / Configure Assessment Questions (Criticality and Control Questions)
- Understand how to Map Criticality Questions to Criticality Risk Levels
- Understand how to Map Control Questions to Criticality Risk Levels
- Understand how to Publish Assessment Questions
- Understand how to Map Assessment Questions to Object Types
- Understand how to Create Assessments (Objects based on the template just created)

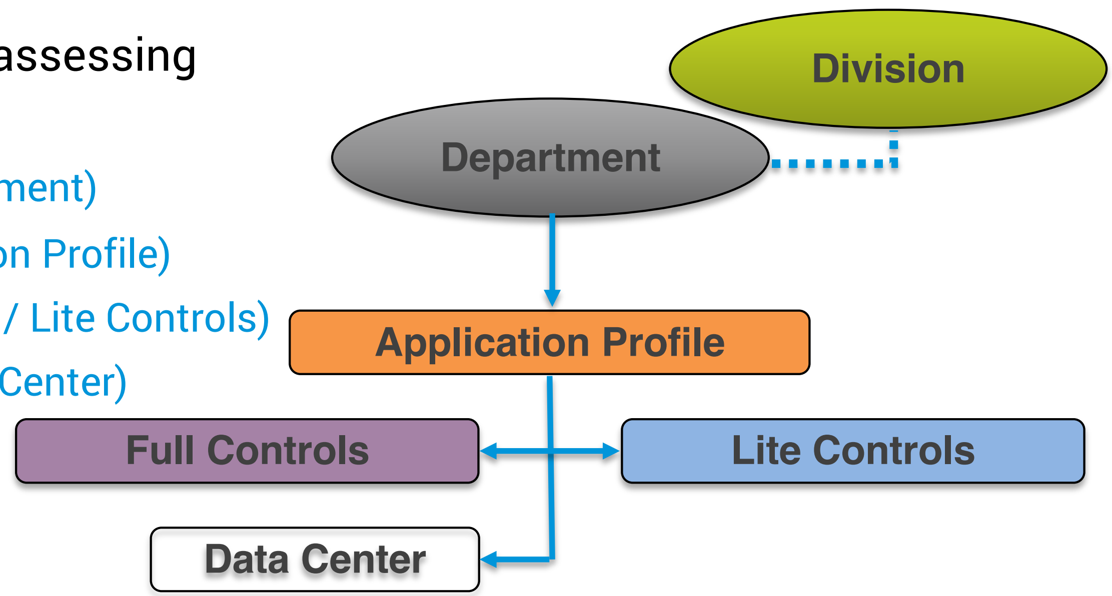
Objects

- Objects
  - Are the primary starting points for most activities
  - Hold all data, Records, Questionnaire Responses and more
  - Can belong to groupings called entities and can have children called Aspects
- Assessment Questionnaires reside at the Object / Aspect level



Understanding Object Types

- Object Types tell Rsam what we are assessing
  - Entities (Object grouping) (Division)
  - Sub-Entity (Object grouping) (Department)
  - Standard (most common) (Application Profile)
  - Aspects (Sub Objects) (Full Controls / Lite Controls)
  - Container (Relational Objects) (Data Center)



Understanding Entity Objects

Entity Objects group Objects together for ease of permission assignment, and data filtering

- Think of Entities as the folders in which objects are stored
- There are two customizable levels of Entities
- Entities are not the only mechanism for grouping. Attributes and Workflow States can also be used for grouping objects in reports / navigation
- Entities are very useful for assigning permissions at a higher level, where they are inherited for all Child Objects and Records
- Entity structures can be changed later, and Objects can be moved into new entities

Examples: Business Unit & Division, Region & Site, Category & Group, Use-Case

Understanding Object Types

Standard Objects represent the heart of the inventory

- Standard Objects are the most common object types
- Standard Objects have all required elements for an assessment
  - Attributes, Controls, and Criticality Factors
- Standard Objects can be either:
  - Self-sustaining OR
  - Relate to other types of Objects
- When in doubt, make it a standard Object type

Examples: Vendor, Data Center, Application

Attribute Types

Control Types

Criticality Factors

Questionnaire Basics

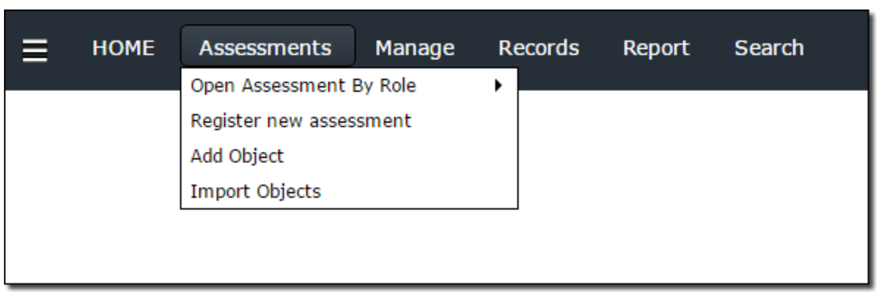
- Two options to create Assessment Questionnaires
- Automatically present the Assessment on creation of an Object
  - Servers supporting Credit Cards automatically get a PCI Assessment
  - Servers support Health Care data automatically get a HIPAA Assessment
- Based on Scoping (Criticality Questions) to drive Assessments
  - What types of data does the Server support?
  - What are the issues of Compromise?
  - General Questions

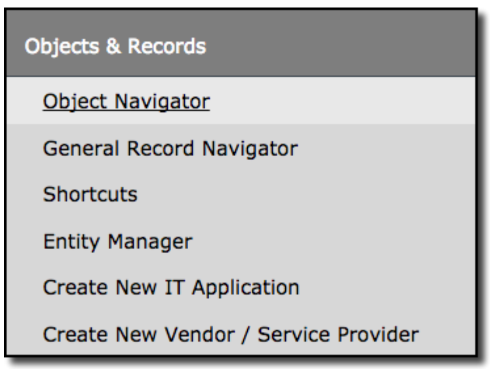
Creating Objects

Galvanize

Objects can be created in many ways:

- Allowing users to click on "Add Object"
- Importing Objects from a data source like Excel or a Database
- Enabling Self Registration
  - Self-Registration allows any user to create a new Object of the specified type without having to be assigned permissions

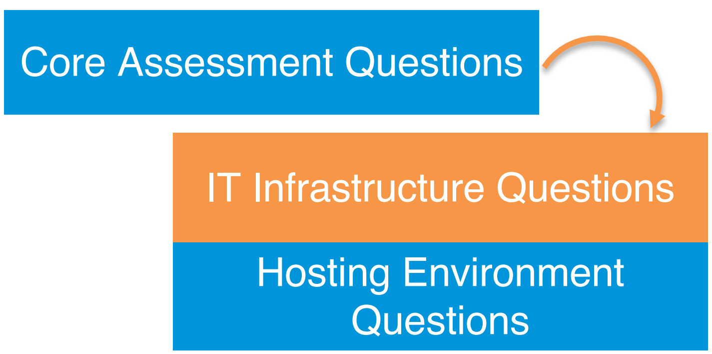




Understanding Aspect Objects

Aspect Objects let you to divide assessments into logical segments vs Standard & Container Objects

- Aspects divide Objects into consistent / logical segments
  - This helps organize data, streamline the process, and permission assignment
- Aspects always belong to other Objects
- Similar to Standard Objects, Aspects can have:
  - Attributes, Controls, Criticality Factors, and Records
- Objects can have multiple Aspects, but only one of each Aspect type



Creating Aspects

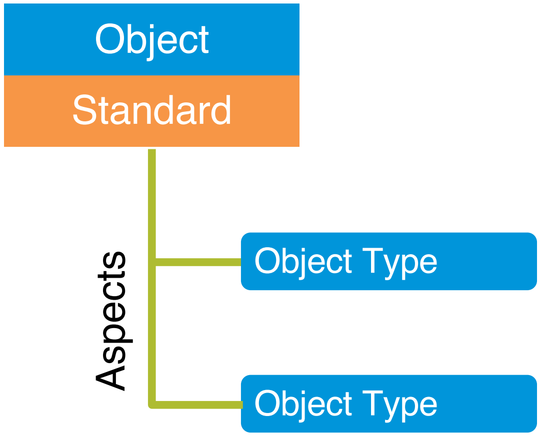
Aspects can be created manually or automatically

- When linking an Aspect Object type to another Object type, you may choose to auto-create that Aspect for all related Objects. This is useful for adding additional context centric questionnaires to all Objects of a specific type
- Aspects can also be automatically created when:
  - user answers a Control or Criticality question in a certain way
  - when clicking a Workflow Button
  - as a Risk Analytics Handler action
- Aspects can also be created manually by users that are given appropriate permissions

Aspect Object Considerations

Aspect Object's Key Considerations

- Aspects divide Objects into logical pieces
- Aspects can add questionnaires to add the baseline
- Aspects get their own questionnaire score but may also be viewed with the total Object score (all Aspects combined)
- Aspects can share Criticality with Standard Objects



Aspect Rules

- Aspects are an optional enhancement (not required)
- Aspects inherit the entity, name, & relationships of the main Object
- Aspect permissions can be "auto inherited" or assigned individually

Creating Objects and Viewing Object Interface

Exercise

Galvanize

Structures and Elements Objects Control and Criticality Questions

Control and Criticality Questions

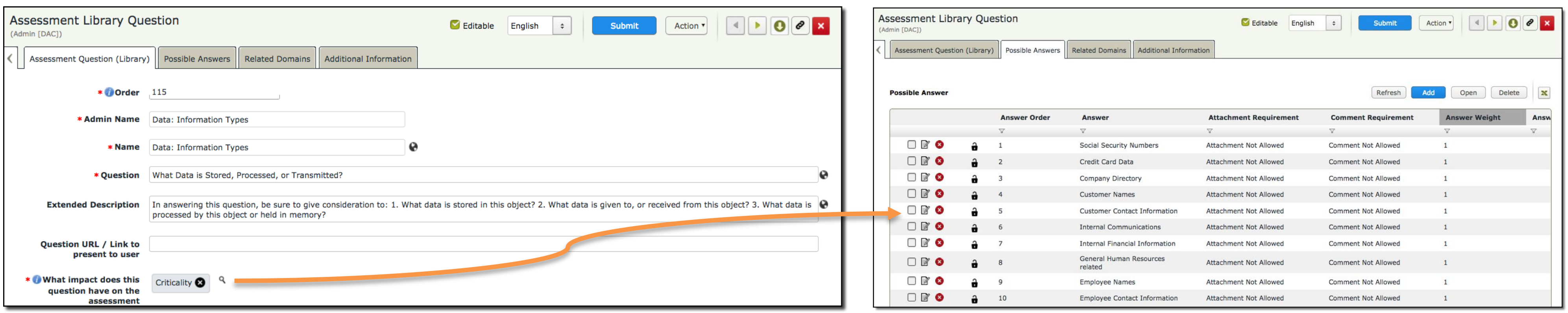
There are two types of question sets used within Assessments / Questionnaires:

- Criticality Based
- Control Based
- Both Types can be assigned to Objects

Criticality Based Questions / Factors

Fact Based Criticality Questions / Factors:

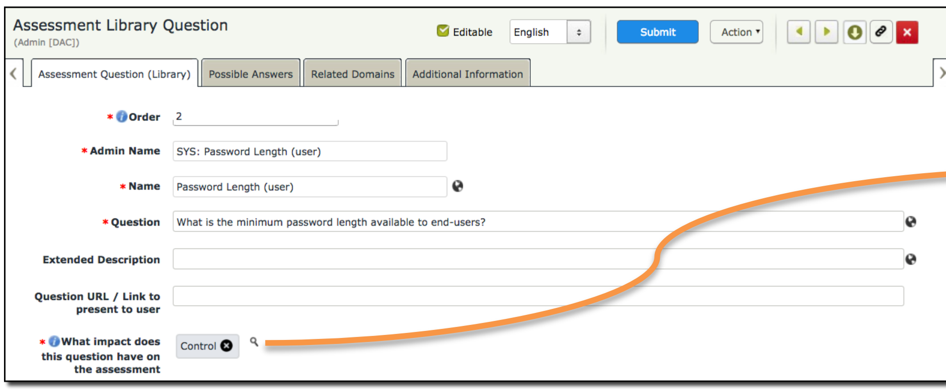
- Help Define the Criticality of a given Assessment
- Rather than asking end-users to rate the importance of Objects (e.g. low, medium, or high), Rsam will prompt for Criticality Questions and then use the data provided to derive these conclusions
- Are one mechanism to drive Aspect creation

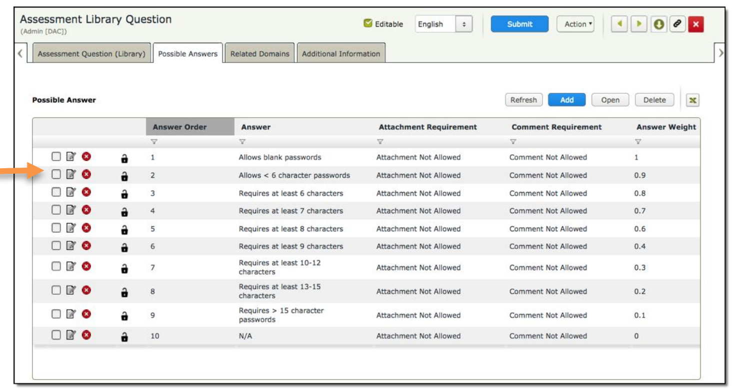


Control Based Questions / Factors

Controls are used to document to what degree a control has been implemented in an object

- Controls consist of both Control Types (the question asked), and Control Levels (possible answers)





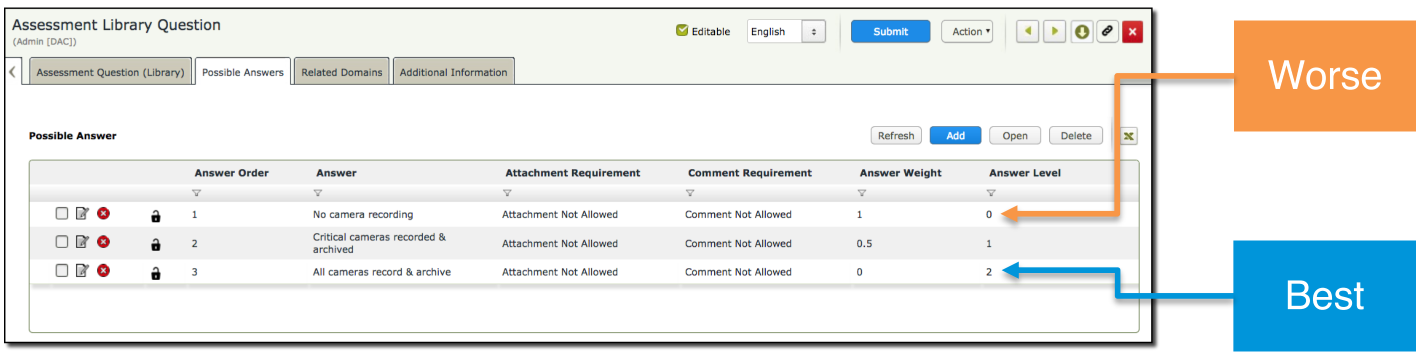
- During reporting & analysis, controls can be measured against standards. Controls failing to meet standards will generate Questionnaire Finding Records and add to the Object's score
- Control Types are associated can be associated with domains to document how the Control relates to regulations, standards, and policies

Controls

Galvanize

Control Levels represent the degrees of control that has been implemented

- Control Levels can be from level 00 to 99
- These levels go in order from 00 representing the least control to 99 representing the most control



Each Answer Level must be equivalent to, or higher than the Answer Level before it

Answer Levels can have several effects on the questionnaire flow, including the ability to:

- Prompt for File Attachments / Evident
- Prompt for Comments / Descriptions
- Define Answer Weights
- Remove other controls from the survey (auto-answers)
- Define Criticality levels
- Generate Aspects

Considerations for Controls

Key Control Considerations

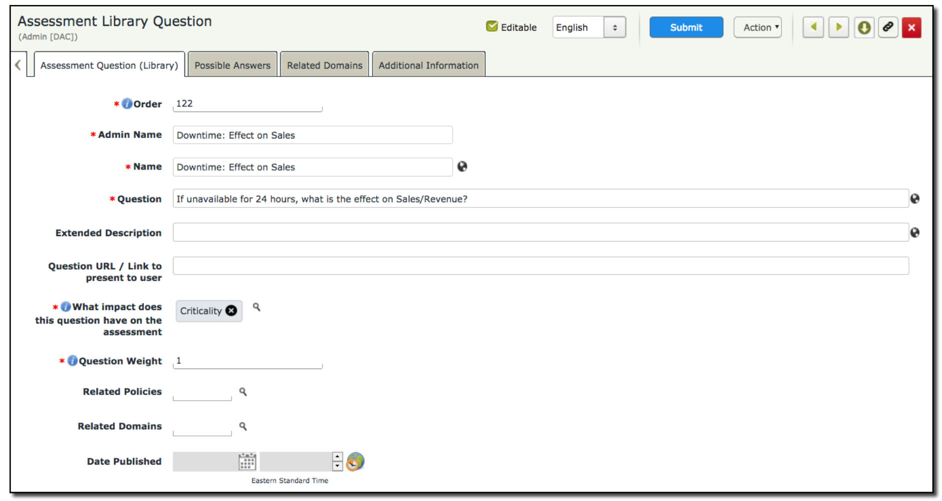
- Each Control Type (Criticality or Control) may be associated with one or more Object Types
- Each Control Type may belong to one or more Domains (data maps)
- Control Types may have hierarchical levels for visual effect
- Control Levels represent increasing degrees of protection

Mapping Control Standards

Galvanize

Control Standards relate Objects to Minimum Control Requirements based on their Criticality

- An Object's criticality is determined by the highest criticality levels from all of its Criticality Factor Questions
- Each Criticality level can have a specific control standard associated with it
- If the Object fails to meet that standard, there is a Gap, a finding record is generated, and points are added to the Object's score



Control Standards

Control Standards can be:

- The same across all levels of criticality (simple assessment), or
- May increase as criticality increases (full assessment)

Required Control levels for: Risks Standards - Standard: Criticality (Security)

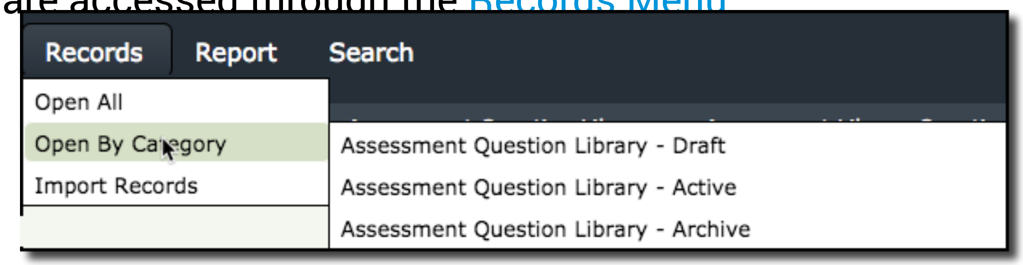
Update Cancel

Control Types	Low	Medium	High	Severe
SYS: Authentication (passwords)	1 :Passwords are used	1 :Passwords are used	1 :Passwords are used	1 :Passwords are used
SYS: Password Length (user)	1 :Allows < 6 character passwords	4 :Requires at least 8 characters	6 :Requires at least 10-12 characters	8 :Requires > 15 character passwords
SYS: Password Aging (user)	0 :Password changes are not forced	1 :Requires annual changes	2 :Requires semi-annual changes	3 :Requires quarterly changes
SYS: Password Complexity (user)	0 :No complexity requirements	2 :Requires 2 alpha, numeric, case, or symbol mix	3 :Requires 3 alpha, numeric, case, or symbol mix	4 :Requires 4 alpha, numeric, case, or symbol mix
SYS: Password History (user)	1 :Restricts re-use of previous 1-2 passwords	2 :Restricts re-use of previous 3-4 passwords	3 :Restricts re-use of previous 5-6 passwords	4:Restricts re-use of previous 7-8 passwords

Publishing Assessment Questions

All assessment questions are created and maintained in Assessment Question Libraries. There are three library categories that correspond to different phases of the assessment question lifecycle.

- Draft – Contains all the questions in the draft form. You can create and update questions from this library.
- Active – Contains all the published and active questions. You can map the questions available in this library to the objects, and the questions appear in the assessments corresponding to the objects.
- Archive – Contains all archived questions corresponding to each question which has been updated. These questions are not used in any active assessments, but can be referenced by older assessments.
- Assessment questions created in Rsam go through a pre-defined lifecycle.
- Question Libraries are accessed through the Records Menu



Library Access

Library Access and Question Management is performed by a number of default accounts

- AQ Editor – This role can Submit questions
- AQ Reviewer – This role can Approve questions
- AQ Manager – This role can Publish questions

When updating existing questions always start from the version of the published question in the Draft library.

Question Library Review & Demonstration
Modifying Object Templates

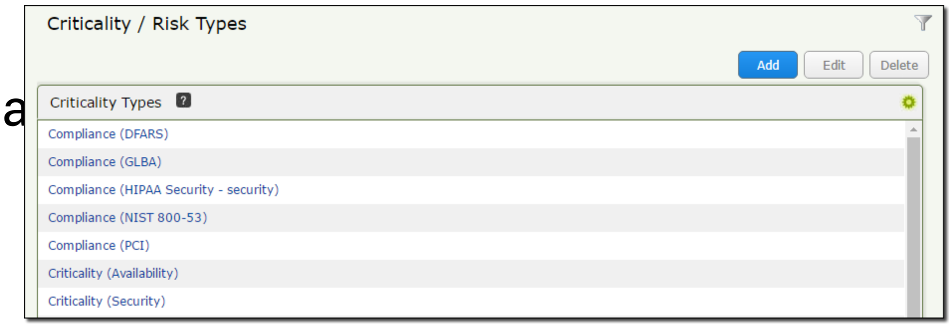
Exercise

Galvanize

Structures and Elements Objects Criticality & Risk Types

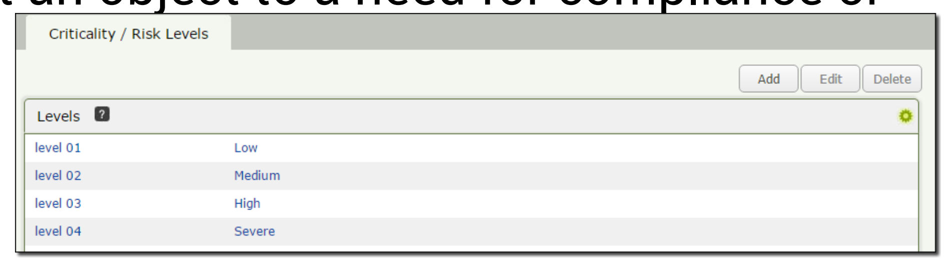
Understanding Criticality Types and Risk Levels

- Criticality / Risk
  Used to show a degree of importance and risk for objects, and to accommoda special handling requirements



- Example
  Availability = Low, Medium or High

- Criticality / Risk
  Can also help relate specific facts about an object to a need for compliance or special handling



- Example
  HIPAA Security Safeguards, GLBA, PCI, Mobile Device, Foreign Connections

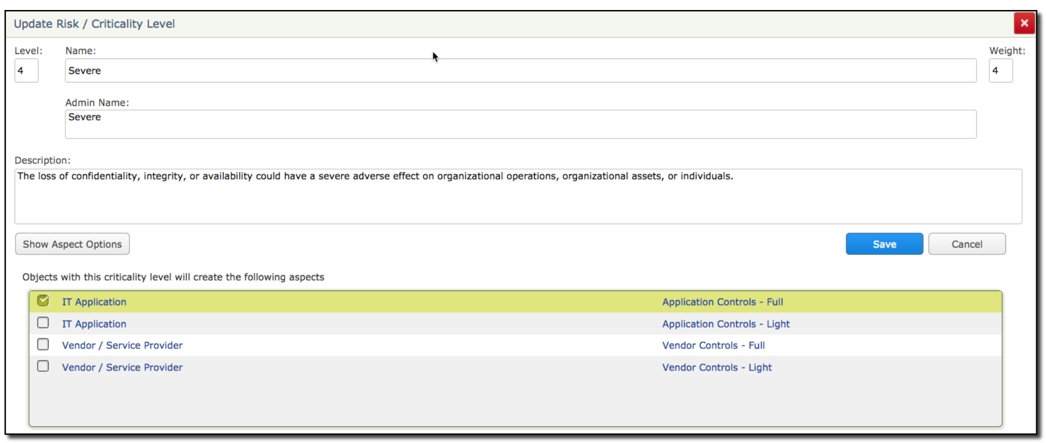
Criticality & Risk

- Criticality / Risk Components have a number of functions
  - Highlight the Criticality and Compliance needed for an object
  - Define the Risk Levels
  - Magnify the score for areas that have higher degrees of risk
  - Align control requirements based on the specific needs of each Object (Control Standards)

Criticality Types / Risk Levels

Criticality Types define the various areas of Criticality / Risk we want the assessment to focus on

- Rsam accommodates up to 100 Criticality / Risk Types
- Each Criticality / Risk Type can have up to 100 related levels, each representing a higher degree of Criticality / Risk
- Risk Levels can drive the creation of Aspect Objects



Galvanize

Demo: Configuring and Creating Criticality Types and Risk Levels

Structures and Elements Objects Scoring

Learning Objectives

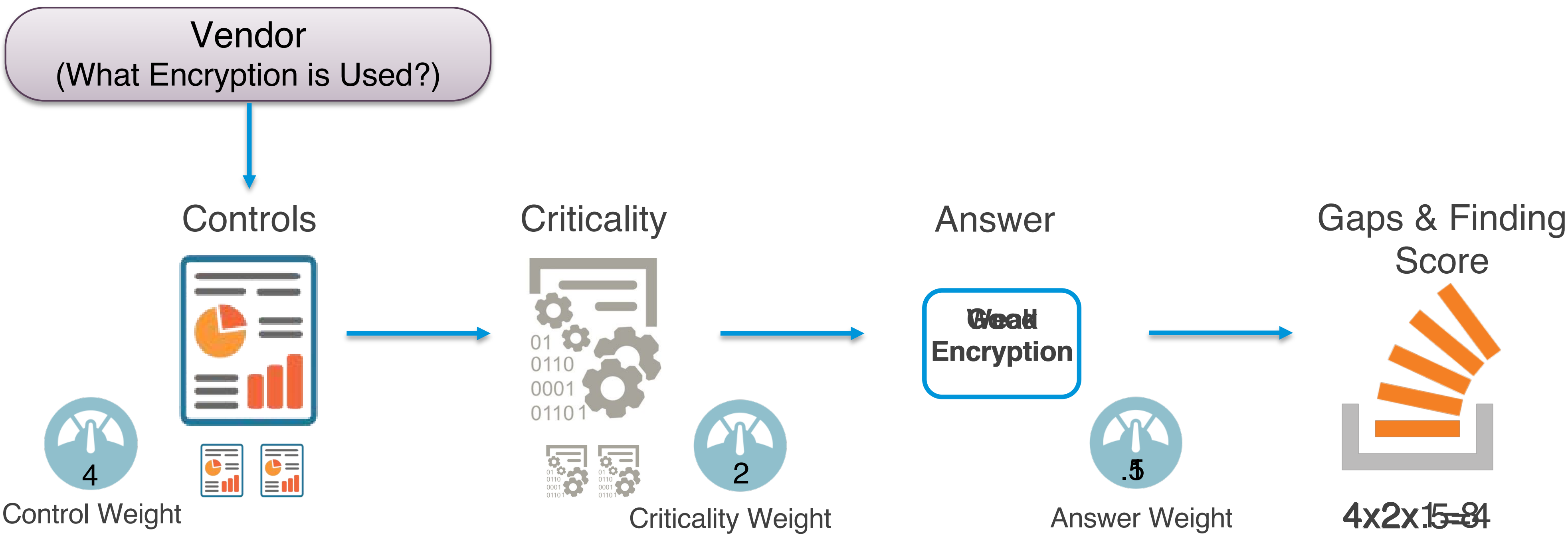
- Understand the purpose behind Rsam scoring
- Identify the components that support the scoring model
- Understand the scoring models available to you

Scoring Engine

Scoring engines create data for analysis and ongoing Risk Management

- Scoring Data fulfills several needs:
  - Helps document findings
  - Draws attention to control priorities
  - Helps direct remediation efforts
  - Helps translate analysis to members of the organization
  - Allows us to track progress/efforts over time

Understanding Object Scores



Understanding Scoring Systems

Object scores are a numeric representation of Risk Control

- “0” is relatively secure; the higher the score, the more in need of attention (Think: Golf Score)
- Points are added when an Object does not meet a recommended standard based on criticality and/or compliance
- Points are magnified by control, criticality, and compliance weights
- Points are also added for container controls

Object Score Calculation

- Example of a Simple Model (All weights = 1 therefore all gaps = 1)
  - (Standard Control Gaps) + (Container Weights)
- Example of a Weighted Model
  - (Standard Control Gaps * Control Weights) + (Container Weights)
- Example of a Risk/Criticality Model
  - (Standard Control Gaps * Control Type Weights * Standard/Compliance Weight)
  - (Container Gaps * Container Weights * Standard/Compliance Weight)

Compiling Gaps

Rsam can compile gaps, taking issues discovered in the questionnaire and generating finding records for them

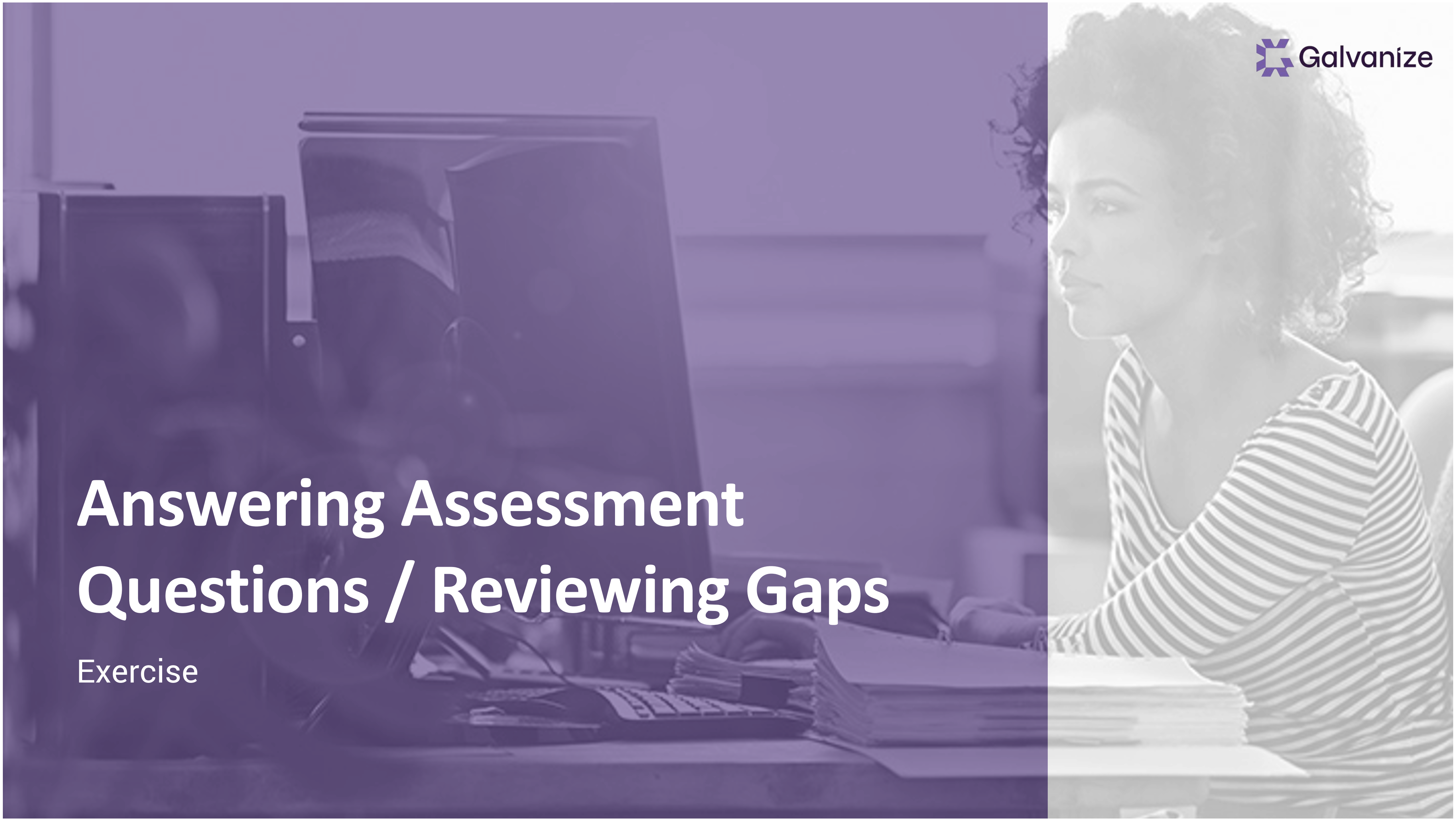
- Customers can elect one or more points in the workflow where Rsam will generate records for each control gap
- Records allow users to then document follow-up items like remediation plans, risk acceptance, and more
- If controls have changed in such a way that a previous gap no longer exists, the record will be archived
- Once compiled, the records are disconnected from questionnaire responses, Records will be updated, or archived when gaps are compiled again

Findings from Questionnaire

Refresh | Add | Open | Delete | Assign...

Instructions

Record Workflow State	Control Name	Supplied Answer	Minimum Required Answer
Open (from questionnaire)	Idle Session Control	Lockout after > 25 minutes	Lockout after 15 - 25 minutes
Open (from questionnaire)	Object Redundancy	Cold Standby	Automatic Failover



Answering Assessment Questions / Reviewing Gaps

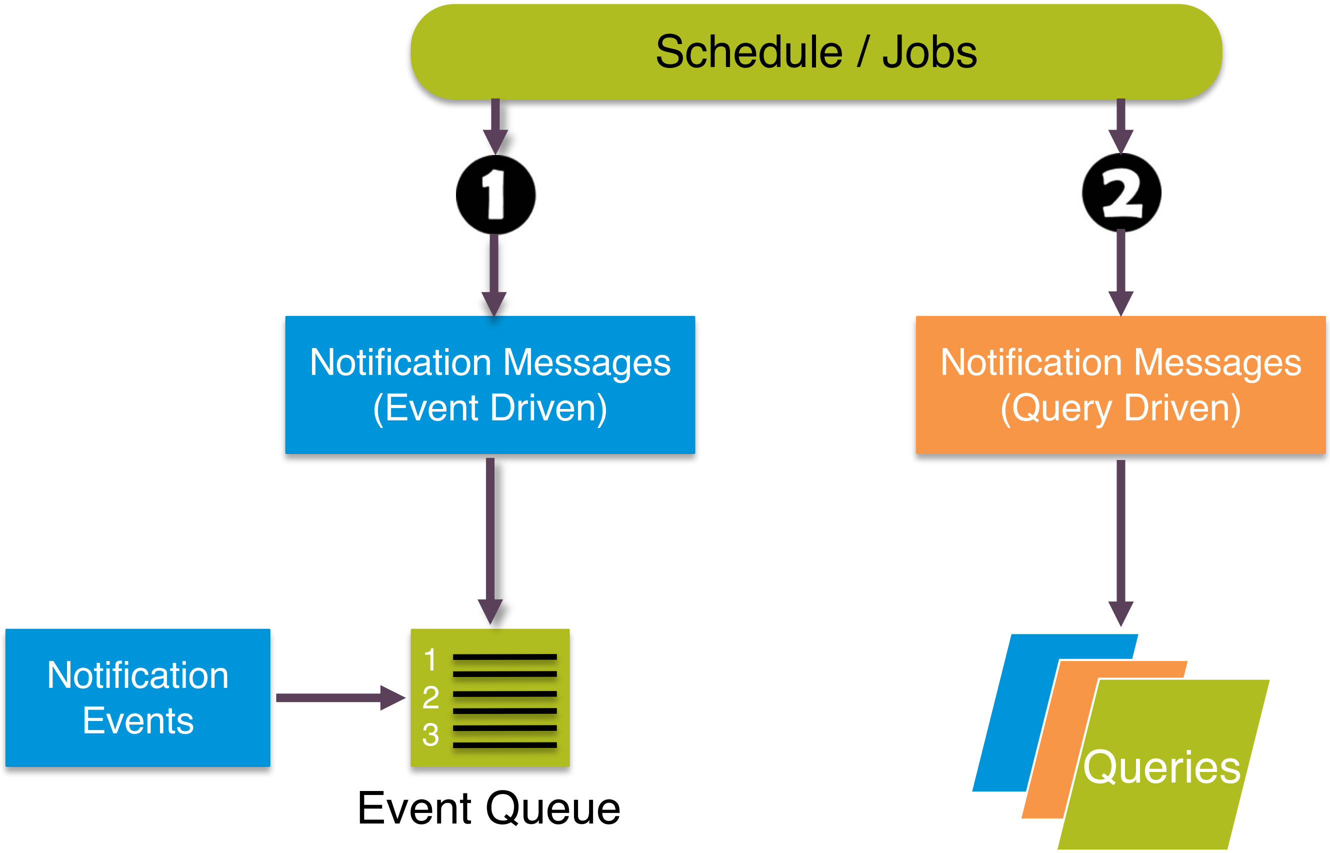
Exercise

Email Notifications

Learning Objectives

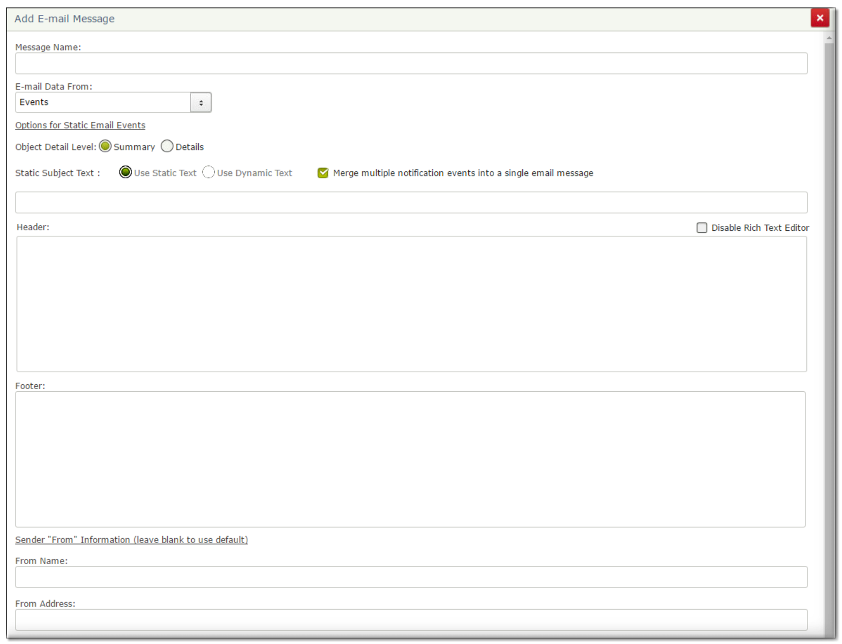
- Understand the purpose behind email notifications
- Identify the different elements that make up email notification
- Understand what can be attached to emails
- Understand how emails and offline decisions co-exist

Notification Components



Notification Message

- Messages define the general wrapper around email notifications
- The message defines the Subject, Header, Footer, and more
- Messages get their actual body content from email Events or Queries

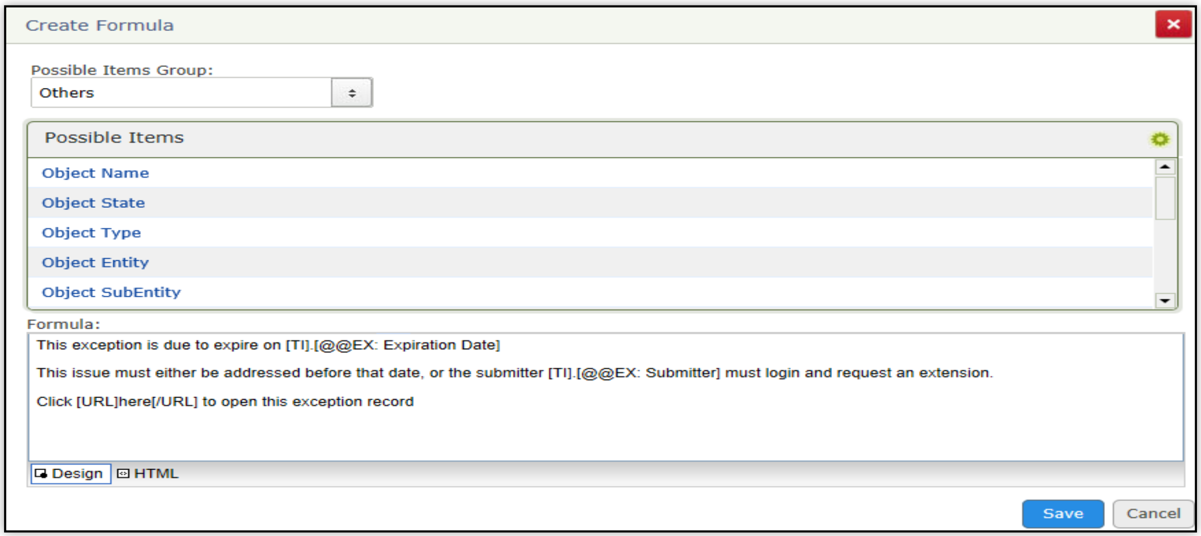


Notification Event

- Events define how event-driven email messages are triggered, what the body of the message will be, and what roles will receive the email message
  - A single email message can be associated with multiple events
- Events have an event Category. The Category determines where the events can be triggered from. The most common categories include:
  - Button Click or Handler: triggered by a user clicking a button or a hander being executed
  - Role Assignment: triggered the moment a user is assigned a role to an object or record

Notification Event (2)

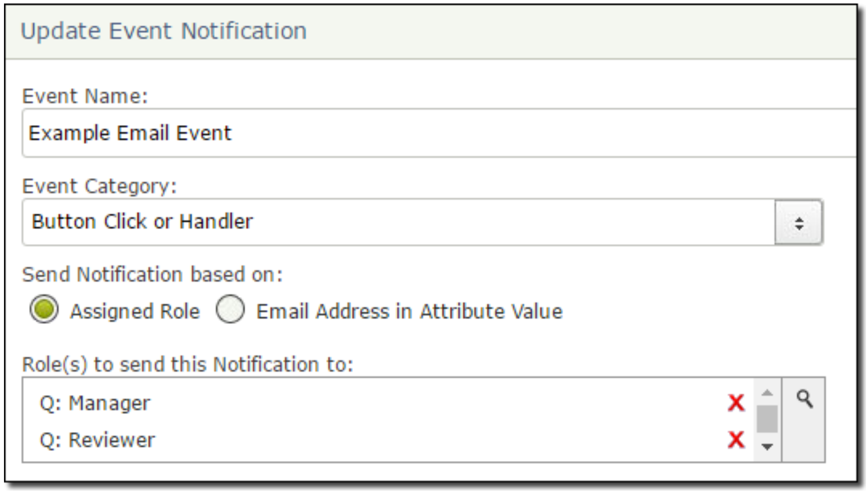
- Event Text is written to the body of the email message. This can be static (the same text every time), or dynamic (defined through formulas that leverage attribute values and other data



- In more advanced use-cases, event text can also be driving from a custom SSRS report. This allows customers to create highly tailored email messages

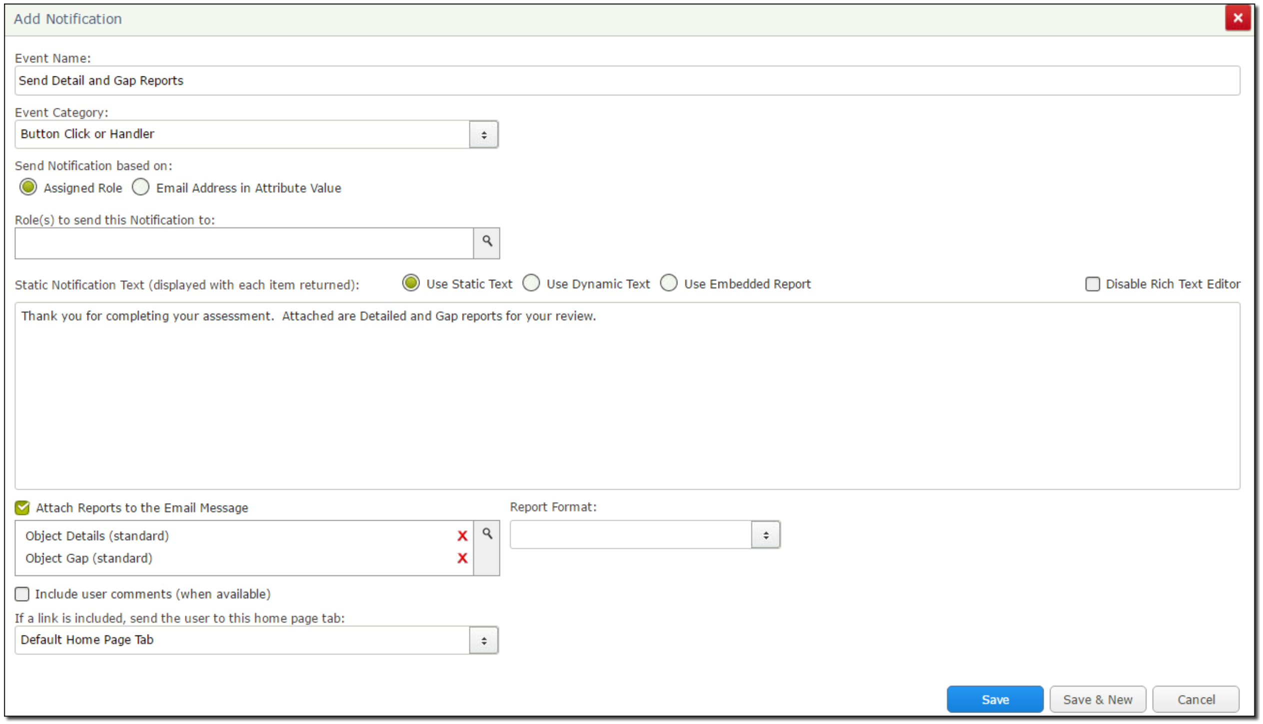
Notification Event (3)

- Event Recipients can be selected via an assigned Role, or via an email address stored in a Text Attribute
  - Role-based Notifications tell Rsam to address the email messages to all users assigned the designated role(s) for the targeted object / record
    - Note that only the users assigned the designated role to the targeted object / record will receive the email. Not users assigned that role to other targets
  - Attribute-based Notifications allow customers to specify who should receive the email by populating an attribute with their email address in the targeted record or object
    - This is very useful for emailing users / accounts that are not assigned roles in Rsam



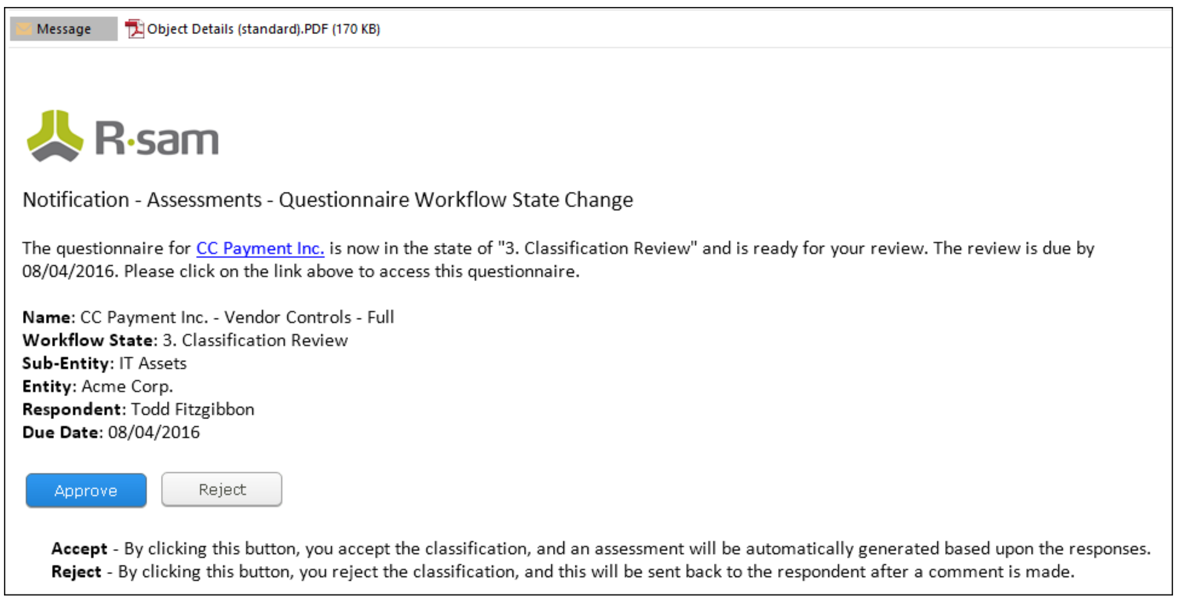
Notification Event (Attach Report File)

- Rsam email event notifications include the ability to attach reports directly to the notification



Notification Event (Offline Decision)

- Rsam also allows you to embed workflow buttons inside of email messages
  - Workflow buttons are selected as a part of the dynamic formula option. This option is available for customers licensed to use offline decision support
- A user receiving the email will simply need to click on the link, authenticate (or complete their single sign-on), and Rsam will automatically execute their selected button



Message | Object Details (standard).PDF (170 KB)

R·sam

Notification - Assessments - Questionnaire Workflow State Change

The questionnaire for CC Payment Inc. is now in the state of "3. Classification Review" and is ready for your review. The review is due by 08/04/2016. Please click on the link above to access this questionnaire.

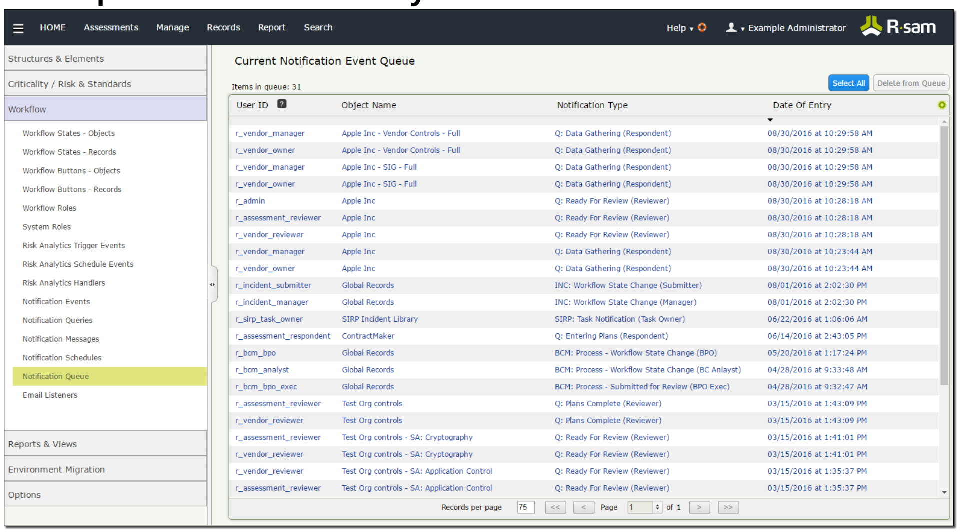
Name: CC Payment Inc. - Vendor Controls - Full
Workflow State: 3. Classification Review
Sub-Entity: IT Assets
Entity: Acme Corp.
Respondent: Todd Fitzgibbon
Due Date: 08/04/2016

Approve | Reject

Accept - By clicking this button, you accept the classification, and an assessment will be automatically generated based upon the responses.
Reject - By clicking this button, you reject the classification, and this will be sent back to the respondent after a comment is made.

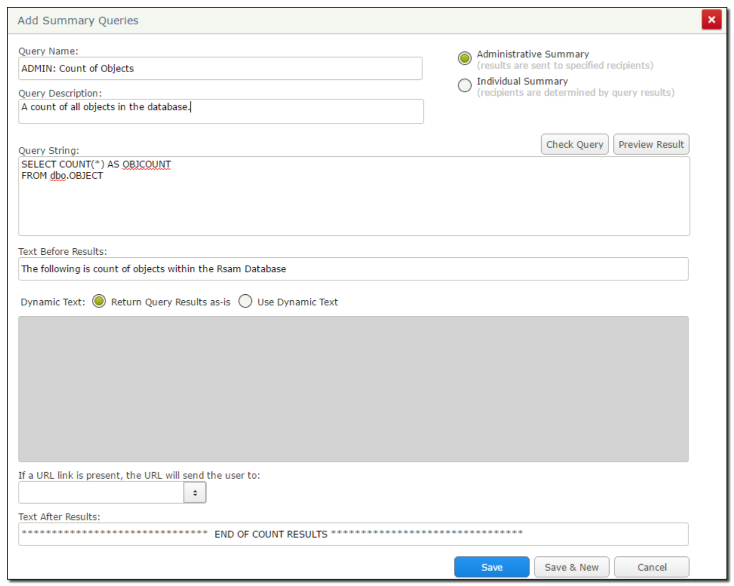
Notification Event (Queue)

- When an email event is triggered, Rsam creates an entry in the Email Queue
- Now Rsam waits for the scheduler related to that event executes, sending out he email messages and clearing them from the Queue
- Administrators can access the queue directly in the Rsam administration screens in order to remove items from the queue before they are sent



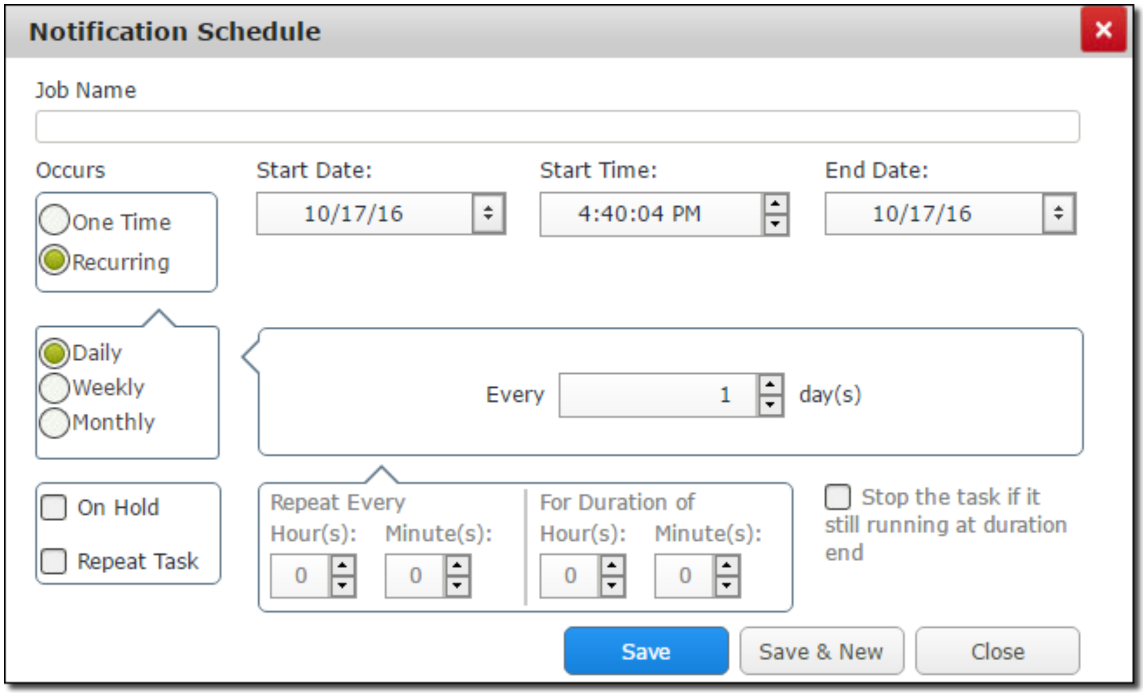
Email Query

- Email messages can also get their data from a SQL Query
- Queries can be leveraged to define more customized messages. Query results are shown in the body of the email message



Notification Job / Schedule

- All notifications are sent out via a schedule
- Schedules can be one-time (on-demand) or recurring



Email Listener

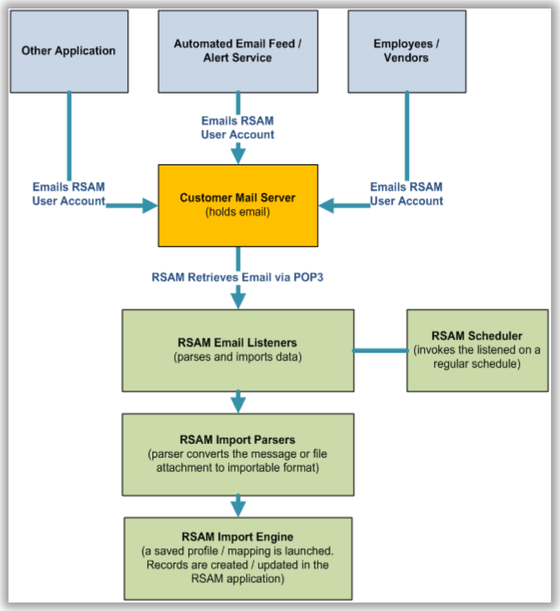
Email Listener

The Email listener allows customers to send information into Rsam using standard email messaging mechanisms

- Customers can use the email listener to Create & Update Objects & Records
- Data can be sent via email in 3 ways
  - As a file attachment
  - As delimited text within the email
  - As a message formatted with pre-defined tags (email elements)

Email Listener Process

- The email listener continually checks a designated POP3 or IMAP email account
- When a message is received, the listener Extracts the data and invokes a saved import profile to Import the data



Email Listener Elements

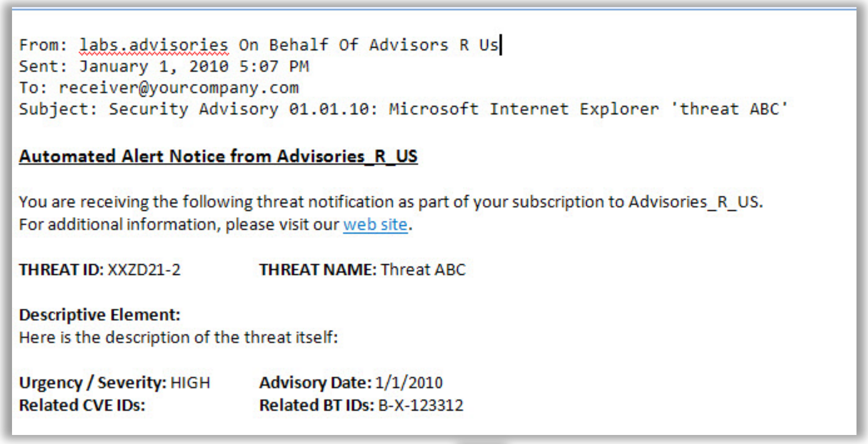
Using Email Elements

- Using email elements allows Rsam to look for specific key words / text in the email message
- Any data that resides between the defined key text elements in considered data
- After specifying the email elements, open the import engine and choose email listener as the data source

Example of Email Listener Elements

Galvanize

Example Email Message


From: labs.advisories On Behalf Of Advisors R Us
Sent: January 1, 2010 5:07 PM
To: receiver@yourcompany.com
Subject: Security Advisory 01.01.10: Microsoft Internet Explorer 'threat ABC'

Automated Alert Notice from Advisories_R_US

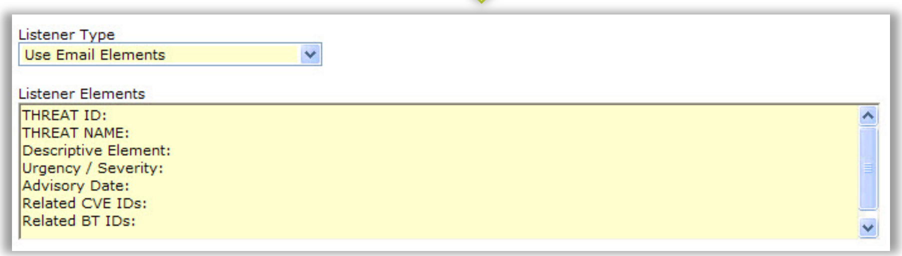
You are receiving the following threat notification as part of your subscription to Advisories_R_US.
For additional information, please visit our web site.

THREAT ID: XXZD21-2 **THREAT NAME:** Threat ABC

Descriptive Element:
Here is the description of the threat itself:

Urgency / Severity: HIGH **Advisory Date:** 1/1/2010
Related CVE IDs: **Related BT IDs:** B-X-123312

Elements



Importable Data

THREAT ID: XXZD21-2

THREAT NAME: Threat ABC

Descriptive Element:: Here is the description of the threat itself:

Urgency / Severity: HIGH

Advisory Date: 1/1/2010

Related CVE IDs:

Related BT IDs: B-X-123312

Galvanize

Thank You