

Governance, Risk and Compliance

Governance, Risk and Compliance



Note: The latest release that this documentation applies to is Fuji. For documentation on the Geneva release, see *Governance, Risk, and Compliance Management* ^[1]. Documentation for later releases is also on docs.servicenow.com ^[2].

Overview

The Governance, Risk, and Compliance (GRC) application supports:

- Downloading and importing UCF authority documents into GRC.
- Documenting policies and procedures.
- Defining and assessing risks.
- Defining controls based on policies and their associated risks.
- Generating audits and tests to ensure that controls are being followed.
- Generating remediation tasks to track corrective actions that are required.



Note: The Core GRC Components [`com.snc.governance_core`] plugin includes components used by the Governance, Risk, and Compliance (GRC) [`com.snc.governance`] plugin. These components include GRC Risks, Risk Criteria, Remediation Tasks, Policies, Standards, and Standard Operating Procedures. The Core GRC Components [`com.snc.governance_core`] plugin **does not include** support for Authority Document management, Unified Compliance Framework (UCF) integration, Control management, Control testing, or Auditing Activities. To leverage these capabilities, install the Governance, Risk, and Compliance (GRC) [`com.snc.governance`] plugin.

GRC Process

The GRC process involves these phases:

- Documentation
- Policy creation
- Monitoring and verification
- Reporting

Documentation

The documentation phase involves creating controls for your Governance, Risk and Compliance audits. Users with the `grc_admin` role can import authority documents from an external standards provider, or create custom controls.

Authority Documents

An authority document is a document that defines the external standards, frameworks, or regulations that a process must use. These are stored as references, from which policies can be defined. Create your own authority documents or download and import the UCF authority documents you want into GRC.

Citations

The authority document can be broken up into *citations* that can be interrelated using configured relationships. In this way, not only can the authority document be viewed as a whole, but the relationships between different sections can be mapped to better record how the authority document is meant to be implemented.

The same relationship mechanism can be used to document relationships across authority documents. This is important because different sources address the same or similar controls and objectives.

Controls

A control is a process to mitigate risk, enforce a mandated policy statement, and address the directive of an authority document. The control may have one or many control tests associated with it. This ensures that the control is effective and provides continued compliance. Controls can also be directly associated with citations to map an organization's internal controls to those mandated by the authority document.

Policy Creation

A policy document defines an internal practice that processes must follow. The Policy [grc_policy] table extends Knowledge [kb_knowledge]. Each policy is stored in the knowledge base and can be accessed in the same way as any other published article.

To manage elements of the policy, the policy can be associated with:

- Entities managed.
- Authority documents with which it is designed to comply.
- Risks associated with failing to comply.
- Controls in place to enforce the policies and mitigate identified risks.

Policy Scope

Scope is the effective level to which a policy, standard, or SOP applies. This could refer to a location, business unit, or anything that is important to the organization. In versions prior to the Fuji release, these levels were called **Entities**.

Monitoring and Verification

Monitoring and verifying the GRC process involves validating controls and tests with audits and evaluating risks.

Risks

A risk is a definition of the possible consequence of failing to comply with a policy. Risks are rated based on risk criteria that can be used to calculate a *risk approach*. The risk approach calculation is based on risk approach rules that typically use the values contained in the **Significance** and **Likelihood** fields in the Risk Criteria [grc_risk_criteria] table. This table contains a **Display value** field to allow for text values and a weighting, which can be used to define the risk approach rules.

After the risks are defined, they can be associated with controls to identify how they are being mitigated.

Control Tests and Definitions

A control test definition determines how and when a control test is performed, including execution steps and expected results. Condition collections can be created with associated conditions to define advanced control test logic. Each time the control test is performed, a control test *instance* is generated as a task to be executed, according to the control test definition.

Audits

An audit definition establishes a set process for validating controls and control tests. From the definition, audit instances can be generated as a task to power the audit.

Once generated, audit instances can reference any existing evidence of compliance by associating previously executed control tests with the control test definitions that have been established in the audit.

During the audit process, audit observations can be recorded by the auditor to track the gathered information. The auditors can use these observations to create remediation tasks.


During the audit process, an administrator can create and assign remediation tasks that need to be performed before and during an audit. In addition, audit requirements associate citations to the audit, allowing auditors to track compliance or non-compliance with the original regulations.

If the latest evidence is not recent enough, click **Execute Now** in the Control Test Definition form to execute a control test instance. This action creates the control test instance and automatically associates it to the audit. The control test instance record also has the **Generate from audit** field populated with the audit number, so that it is clear that the test was created from an audit and not manually.

Reporting

GRC provides three reporting portals that deliver reports to specific users related to the GRC elements assigned to them or their groups.

Menus and Modules

	<ul style="list-style-type: none"> • My GRC: Displays all available GRC reports in the portal to users with the <code>grc_admin</code> role. This module is available starting with the Fuji release. • My GRC Audits: Displays all available audit reports in the portal to users with the <code>grc_audit_definition_admin</code> or <code>grc_internal_auditor</code> role. This module is available starting with the Fuji release. • My GRC Controls: Displays all available control reports in the portal to users with the <code>grc_test_definition_admin</code> or <code>grc_process_owner</code> role. This module is available starting with the Fuji release. • Policies: Displays a list of policies that contains documents describing internal practices that processes must follow. • Standards: Displays a list of standard policy classes that you can use to define policies at a specific level in an organization. • Standard Operating Procedures: Displays a list of standard operating procedure (SOP) policy classes that you can use to define policies at a specific level in an organization. • Risks: Displays a list of risks that define the potential consequences of ignoring policies. • Controls: Contains modules that display all controls or those controls associated with the logged in user or the logged in user's group. • Control Tests: Contains modules that display all control tests or those tests associated with the logged in user or the logged in user's group. • Remediation: Contains modules that display all remediation tasks or those tasks associated with the logged in user or the logged in user's group. • Audit: Contains modules that display all audits or those audits associated with the logged in user or the logged in user's group. Also displays an Overview portal containing audit-related reports. • Observations: Contains modules that display all audit observations or those observations associated with the logged in user or the logged in user's group. • Authority Documents <ul style="list-style-type: none"> • Authority Documents: Displays the list of authority documents. • Citations: Displays the list of citations. • Relationship Types: Displays the list of the relationships that exist between citations. • Administration <ul style="list-style-type: none"> • Scopes: Displays the list of scopes that define the various levels available for policies, standards, and SOPs. In versions at Eureka and earlier, this module is called Entities. • Risk Criteria: Displays the list of risk criteria. • Risk Approach Rules: Displays the list of risk approach rules. • Control Test Definitions: Displays the list of control test definitions. • Condition Collections: Displays the list of condition collections. • Conditions: Displays the list of predefined conditions. • Audit Definitions: Displays the list of audit definitions. • Filters: Displays the list of active certification filters. This functionality is available starting with the Dublin release. • Templates: Displays the list of certification templates of audit type Compliance. This functionality is available starting with the Dublin release. • UCF Update Status: Displays the status of the last UCF update, by phases. This module is available starting with the Fuji release. • Import UCF Content: Initiates the download or update of UCF authority documents. Download or update UCF authority documents and select content for import into GRC tables. This module is available starting with the Fuji release. • Properties: Displays the GRC properties, including UCF import settings. This module is available starting with the Fuji release.
--	---

Activating Governance Risk and Compliance

Administrators can activate the Governance, Risk and Compliance plugin. Additional plugins are activated as needed. This plugin provides demonstration data.



Note: The Core GRC Components [com.snc.governance_core] plugin includes components used by the Governance, Risk, and Compliance (GRC) [com.snc.governance] plugin. These components include GRC Risks, Risk Criteria, Remediation Tasks, Policies, Standards, and Standard Operating Procedures. The Core GRC Components [com.snc.governance_core] plugin **does not include** support for Authority Document management, Unified Compliance Framework (UCF) integration, Control management, Control testing, or Auditing Activities. To leverage these capabilities, install the Governance, Risk, and Compliance (GRC) [com.snc.governance] plugin.

Click the plus to expand instructions for activating a plugin.

If you have the admin role, use the following steps to activate the plugin.

1. Navigate to **System Definition > Plugins**.
2. Right-click the plugin name on the list and select **Activate/Upgrade**.

If the plugin depends on other plugins, these plugins are listed along with their activation status.

3. [Optional] If available, select the **Load demo data** check box.

Some plugins include demo data—sample records that are designed to illustrate plugin features for common use cases. Loading demo data is a good policy when you first activate the plugin on a development or test instance. You can load demo data after the plugin is activated by repeating this process and selecting the check box.

4. Click **Activate**.

Enhancements

Fuji

- GRC supports the use of UCF authority documents in GRC authority documents, citations, and controls. Administrators use a dedicated interface to select and import specific authority documents that contain the guidance they need. GRC tracks UCF versions and enables administrators to view changes before importing a new version of a document. An approval process ensures that only those documents currently used by the organization for compliance are imported into GRC tables.
- A type of survey called an attestation allows an organization to evaluate its compliance with its policies. An attestation is created in a control test definition and sent to users who execute company policy or manage compliance standards. GRC gathers and displays results from each control test based on the configured scoring criteria. Administrators can create an *assertion* on the attestation that contains requirements, admonitions, or directions related to the questions, and then require recipients to certify that they have read and complied with the policy with a signature.
- Attestation scorecards display the responses from each survey by recipient, question, or category and provide yearly or quarterly comparisons. Scorecards are dynamically updated by the system.
- GRC provides reporting on compliance, controls, and audits. Audit reports are driven by database views, which enable reporting on joined tables. Three report portals deliver reports to specific users, by role, related to the GRC elements assigned to them or their groups.
- The system automatically generates calculated links between authority documents, citations, policies, and risks in any hierarchy you establish. This feature creates indirect links between GRC elements that update dynamically and enable the system to roll up results from control tests for reporting purposes.
- GRC automatically executes any control test definition associated with an audit definition when the audit instance is created.

Dublin

- Control test definitions support the use of certification filters and templates to define the scope and conditions for control tests. Templates enable an administrator to define attribute conditions for any table in ServiceNow.
- Demonstration data provided with the Dublin release enables customers to audit vendors for non-disclosure agreements (NDA). You can substitute filters and templates for the existing condition collection functionality, but you must create your own records. ServiceNow does not provide NDA demonstration data for the new elements.

References

[1] https://servicenow.suiteshare.net/bundle/geneva-it-business-management/page/product/it_governance_risk_and_compliance/reference/grc-landing-page.html

[2] <https://docs.servicenow.com/>

Defining Authoritative Sources

Overview

An *authority document* is a document which defines external standards, frameworks, or regulations that process must follow. Each authority document is defined by a master record on the Authoritative Source [grc_authoritative_source] table, with a related list of records from the Authoritative Source Content [grc_authoritative_src_content] table. These *citation* records contain the actual provisions of the authority document, which can be interrelated.

Use these authority documents, to define policies, risks, controls, audits, and other processes to ensure adherence to the authoritative content.

Field	Description
Name	Name of the UCF document imported into GRC.
URL	[Read-only] Link to the authority document on the original site that contains this authority document. This field is available starting with the Fuji release.
Type	Document type. The default type for all UCF imports is Standard .
Source	[Read-only] Source of the data in this authority document. For all records imported from UCF, UCF is the value. This field is available starting with the Fuji release.
Source ID	[Read-only] Internal unique UCF identifier for this authority document. This value is inherited from UCF when the document is imported. This field is available starting with the Fuji release.
Source version	[Read-only] Version of the UCF authority document that is the source file for this authority document. Previous versions of this authority document are listed in the Other versions related list. This field is available starting with the Fuji release.
Version	[Read-only] Version number for previous versions of this authority document. This value is a simple integer that is incremented by the system each time the UCF authority document is updated. This number is not the same as the UCF Source version . The Version field is hidden when the current version of the record is displayed. You can view all available versions by selecting records from the Other Versions related list. For more information, see UCF Authority Document Versions. This field is available starting with the Fuji release.
Coverage	[Read-only] Number of UCF controls linked to this authority document that have control test instances. This field is available starting with the Fuji release.
Compliance	[Read-only] Number of compliant control test instances associated with this authority document. This field is available starting with the Fuji release.
Non-compliance	[Read-only] Number of non-compliant control test instances associated with this authority document. This field is available starting with the Fuji release.
Pertinent	Indicates if an imported UCF authority document is relevant to your organization. By default, this check box is selected and has a value of True . Clear this checkbox to mark this authority document as not pertinent to your organization and to prevent it from appearing in compliance reporting. This field is available starting with the Fuji release.
Additional information	Information of any type that is pertinent to this authority document. This field is available starting with the Fuji release.

UCF Authority Document Versions

The ServiceNow system creates a new version of an authority document each time a new UCF authority document is imported into GRC. When a new version of an authority document is created, the system adds the previous version to the **Other versions** related list in the Authority Document form. These records are used for reference only and provide a history of how each version of the UCF authority document was used. New control tests run against the current control version only. Only the latest version of each authority document appears in lists.

Deleting Authority Documents

You cannot delete a GRC record that has a linked dependency to another GRC record. The **Delete** button appears in records and record lists, but only *deactivates* the entity rather than removing it from the system. Deactivation clears the **Pertinent** check box in the record, which removes any links to other GRC entities. By default, deactivated records are filtered out of related lists. Manually created GRC records with no linked dependencies can be completely deleted from the system. UCF records imported into GRC tables can only be deactivated. Only users with the admin role can deactivate or delete GRC records.

References

[1] <http://www.unifiedcompliance.com/>

Managing Policies

Overview

A GRC *policy* is a document which defines an internal practice that processes must follow. The Policy [grc_policy] table extends Knowledge [kb_knowledge], so each policy is stored in the knowledge base and can be accessed in the same way as any other published article. GRC offers two additional policy classes called Standards and Standard Operating Procedures (SOP), that you can use to define specific practices at different levels within an organization. These two classes are available starting with the Fuji release.

These records can be associated with:

- Scopes that define the level for which a policy class applies.
- Authority documents and citations to which a policy class applies.
- Risks associated with failing to comply.
- Controls in place to enforce the policy class and mitigate identified risks.

Defining Policies by Class

The tables for standards and standard operating procedures (SOP) extend the Policy [grc_policy] table and provide the same information. You can use standards and SOPs to apply GRC policies to specific levels or scopes within an organization. For example, a scope can be an installation in another state that is subject to different regulations or a department that has to meet specific requirements.

You can create a policy, standard, or SOP from one of these locations:

- **GRC > Policies**
- **GRC > Standards**
- **GRC > Standard Operating Procedures**



Note: Records for all classes are available in the Policies record list, but only standard and SOP records appear in their respective lists.

Policy - Non-Disclosure Agreements (NDAs) are required for all vendors

Number: KB0009032 Published: 2015-01-03

Workflow: Published Valid to: 2021-07-10

Article type: HTML Parent policy:

Attachment link: ☐ Compliance:

Image: ☐ Non compliance:

Pertinent: ☐ Roles:

* Short description: Non-Disclosure Agreements (NDAs) are required for all vendors

Text: All vendors must have a valid, active NDA in place for us to do business with them.

Additional information:

Mark Public Update Delete

Related Links

View Article

Scope Authority Documents Citations Controls (1) Policies Risks

Controls New Edit... Go to Control Search

Policy - Non-Disclosure Agreements (NDAs) are required for all vendors

Control All vendors must have a Non-Disclosure agreement

Connected by (empty)

Actions on selected rows...

Field	Input Value
Number	A unique number assigned to the KB article using Number Maintenance.
Workflow	A stage field for how far along the policy is in the drafting process.
Article type	The type of markup used to write the article. Choices are HTML and Wiki .
Attachment link	Indicator that, if selected, opens the attachment rather than opening the policy in the Knowledge Base when the user selects the policy from the Knowledge Base.
Image	An icon to appear next to the policy in the Knowledge Base.
Pertinent	Indicator that determines if a policy is relevant to your organization. By default, this check box is selected. Clear this checkbox to mark this policy as not pertinent to your organization and to prevent it from appearing in compliance reporting. This field is available starting with the Fuji release.
Published	Date of publication.
Valid to	A date for the Policy to no longer appear in the knowledge base.
Parent policy	Reference field identifying a policy that is a parent to this policy. You can establish parent/child relationships between policies, standards, and standard operating procedures (SOP).
Compliance	[Read-only] Percentage of compliant control test instances associated with this policy. This field is available starting with the Fuji release.
Non compliance	[Read-only] Percentage of non-compliant control test instances associated with this policy. This field is available starting with the Fuji release.
Roles	The user roles required for users to see the article. If empty, <i>everyone</i> can see the policy. Once a role is input, only the selected roles can see the policy.
Short Description	[Required] A unique description or title for this policy, standard, or SOP. The system displays this value for selection when you add link policies to a GRC entity record in the Policies related list. Make sure to provide a clear description that differentiates it from other policies, standards, or SOPs.
Text	The text of the policy, written in the appropriate markup language for the specified Article type .

Additional information Information of any type that is pertinent to this policy. This field is available starting with the Fuji release.

Fields visible for versions prior to Fuji

Classification A choice list of how the article is classified, specific to policies.

Distribution A choice of how the policy is to be distributed.

Topic The topic that determines where in the Knowledge Base the policy appears. By default, this value is **Policies**.

Defining Scope

Scope is the effective level to which a policy, standard, or SOP applies. For example, you might apply a standard at the company level and then create an SOP for an organizational unit within the company. You define entities using these types in the Scope [grc_entity] table and apply them to a policy class in the **Scope** related list. In versions prior to the Fuji release, the **Scope** module was called **Entities**.

The following scope types are provided in the base GRC system:

- **Location**
- **Business Area**
- **Operational Classification**

To define a scope, navigate to **GRC > Administration > Scopes** and click **New**. Give your scope a unique and descriptive name and select a **Type** representing the level you need for a particular policy class.

Enforcing Policies

After policies are defined, there are two processes available for ensuring that their provisions are followed:

- **Risk Managing** - After risks are defined, they can be managed using Controls and Control Tests to protect against the consequences of breaching policies.
- **Audits** - After all the processes for policies have been defined, audits can be performed to confirm that they are being performed properly.

Defining Risks

Overview

A *risk* is a defined consequence that can occur if a policy is ignored. After risks are defined, they can be managed by:

- Defining Risk Criteria
- Defining Risk Approach Rules
- Creating Controls
- Creating and performing Control Tests

Defining a Risk

To define a Risk, navigate to **GRC > Risks** and click **New**. Populate the following fields:

Field	Input Value
Risk ID	A unique number assigned to the Risk using number maintenance.
Risk Name	The name of the risk.
Significance	The impact of the the risk if it is realized. Defined by Risk Criteria.
Likelihood	The probability that the risk will be realized. Defined by risk criteria.
Recommended approach	A reference to the Risk Approach Rule that determines how to treat this risk. Can be calculated dynamically using the Calculate Risk Approach UI action on the form.
Pertinent	Indicator that shows if a risk document is relevant to your organization. By default, this check box is selected and has a value of True . Clear this checkbox to mark this risk as not pertinent to your organization and to prevent it from appearing in compliance reporting. This field is available starting with the Fuji release.
State	A choice field for the state of the risk. Choose from: <ul style="list-style-type: none"> • Known – The existence of the risk is known. This is the default value. • Open – The risk has been analysed. • Issue – The risk has occurred. • Closed – The risk is no longer valid. For example, the risk was related to mainframes, but the organization no longer uses mainframes.
Category	What category of risk applies to the record.
Compliance	[Read-only] Percentage of compliant control test instances associated with this risk. This field is available starting with the Fuji release.
Non-compliance	[Read-only] Percentage of non-compliant control test instances associated with this risk. This field is available starting with the Fuji release.
Applies To	A Document ID field to identify the scope.
Description	A verbose description of the risk.
Additional information	Information of any type that is pertinent to this risk. This field is available starting with the Fuji release.

Defining Risk Criteria

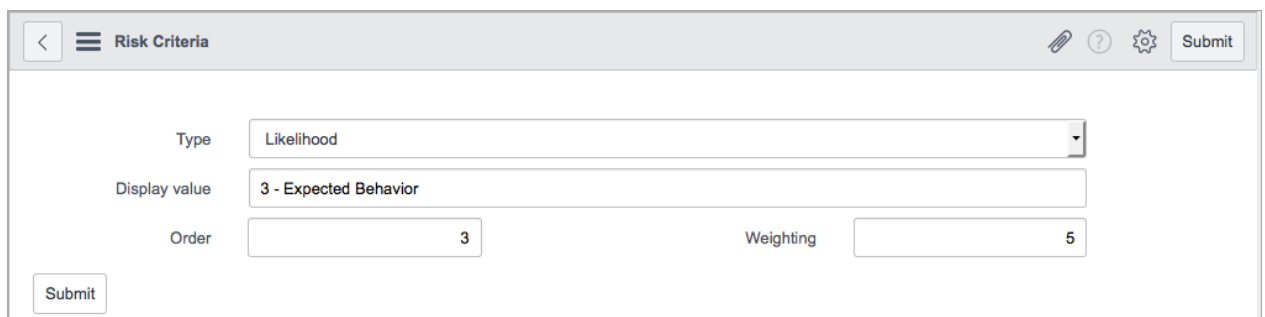
In the base GRC system, the available risk criteria types are:

- **Significance**
- **Likelihood**

Values for these types are stored in the Risk Criteria [grc_risk_criteria] table. Demo data in GRC provides a default range of criteria levels from least to most for both types. Starting with the Fuji release, you cannot create new risk criteria types.

To create risk criteria:

1. Navigate to **GRC > Administration > Risk Criteria**.
2. Click **New**.
3. Complete these fields:
 - **Type:** Select one of the types provided, either **Likelihood** or **Significance**.
 - **Display value:** Create a name for the criteria that displays in the choice list. For example, enter **3 - Expected Behavior** for the **Likelihood** type.
 - **Order:** The order in which this choice appears in the choice list. This order should be logical for the level selected.
 - **Weighting:** A numeric value for the risk, used to calculate risk approach rules. Low weighting factor indicates a lower overall risk, and high weighting factor indicates a higher overall risk.
4. Click **Submit**.



The screenshot shows the 'Risk Criteria' form in the GRC system. The form has a header bar with a back arrow, a menu icon, the title 'Risk Criteria', and icons for a paperclip, help, settings, and a 'Submit' button. The form fields are: 'Type' (a dropdown menu with 'Likelihood' selected), 'Display value' (a text field containing '3 - Expected Behavior'), 'Order' (a text field containing '3'), and 'Weighting' (a text field containing '5'). A 'Submit' button is located at the bottom left of the form.

5. To select the new criteria in a risk record, navigate to **GRC > Risks** and click **New**.
6. Open the choice list for the **Likelihood** field.

The new criteria appears in the list by its display name.

The screenshot shows a 'Risk' form with the following fields and values:

- Risk ID:** RISK0002002
- Name:** (empty)
- Significance:** -- None --
- Likelihood:** -- None -- (dropdown menu is open showing options: 5 - Extremely Likely, 4 - Improbable, 3 - Expected Behavior, 4 - Unexpected, 2 - Unknown, 1 - Unlikely)
- Recommended approach:** (empty)
- Pertinent:** (empty)
- Description:** (empty)

Defining Risk Criteria in Versions at Eureka and Earlier

Click to expand

Risk criteria are defined on the Risk Criteria [grc_risk_criteria] table, which holds a record for each possible choice, grouped by **Type**. In the base GRC system, demo data is provided for these risk criteria types:

- **Significance**
- **Likelihood**

You can create new types or create new risk criteria for existing types. For risk criteria with custom types to be available on the Risk form, you must add a new field for that type to the form and configure it to show your risk criteria choices.

To create risk criteria:

1. Navigate to **GRC > Administration > Risk Criteria**.
2. Click **New**.

Populate the fields as follows:

- **Display value:** One of the choices for the new Risk Criteria (e.g. **5 - Extremely Expensive**).
- **Order:** The order in which this choice appears in the choice list.
- **Type:** The name of a new risk criteria type, such as **Cost**.
- **Weighting:** A numeric value for the risk, used to calculate Risk Approach Rules. Low **Weighting** indicates a lower overall Risk, and high **Weighting** indicates a higher overall risk.

The screenshot shows the 'Risk Criteria' form with the following fields and values:

- Weighting:** 5
- Order:** 5
- Type:** Cost
- Display value:** 5 - Extremely Expensive

There is a 'Submit' button at the bottom left of the form.

3. Repeat the previous step for each of the choices for the new risk criteria. Keep the **Type** field the same, while changing the other fields appropriately to create a range.

4. Navigate to **GRC > Risks**.
5. Open an existing risk definition record or click **New** to create one.
6. Configure the form to add a new reference field to the **Risk Criteria** [grc_risk_criteria] table.

Typically, this new field should share the same name as the **Type** you created for the risk criteria. In this case, use **Cost**.

7. Right-click the new field's label and select **Personalize Dictionary**.
 1. For the **Reference qual condition** field, add [Type] [is] [<type value>], where <type value> is the value from the **Type** field in the risk criteria record. In this example, the condition is [Type] [is] [Cost]
 2. To format the field as a choice list, select **Drop-down with --None--** from the **Choice** field.
 3. Click **Submit**.

The new field appears on the form as a choice list.

8. Display the choice list to see the available criteria.

The screenshot shows a web form for defining risks. It includes the following fields and their current values:

- Significance:** 10 - Major Significance
- Likelihood:** 3
- Recommended approach:** Prevent at Source
- Cost:** A dropdown menu is open, showing the following options:
 - ✓ -- None --
 - 1 - Insignificant
 - 2
 - 3
 - 4
 - 5 - Extremely Expensive (highlighted)

A **Submit** button is located below the Cost field.

Defining Risk Approach Rules

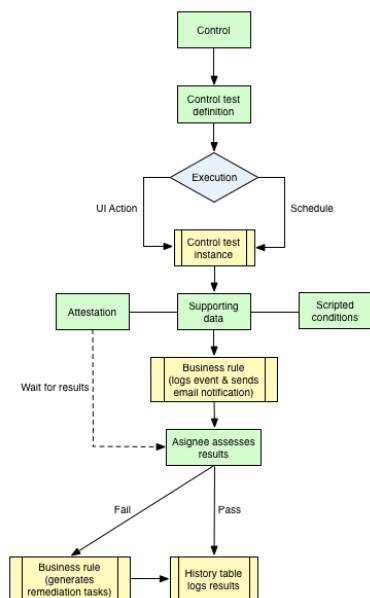
To define a risk approach rule, navigate to **Governance, Risk, & Compliance > Risk Approach Rules** and click **New**. Populate the following fields:

Field	Input Value
Recommended approach	A short description of the approach philosophy that will be used to mitigate the risk.
Active	If checked, the approach will be available for selection.
Condition	A condition builder that determines what risks to which this approach is applied when the Calculate Risk Approach button is clicked. Note: the first condition that is matched wins, so when creating new risk approach rules ensure that the conditions do not overlap with other risk approaches.
Description	A full description of the risk approach.

Managing Controls and Tests

Overview

After you identify the risks, define controls or import them from UCF authority documents and then create control test definitions to prevent issues from occurring. This diagram illustrates the entire GRC control process.



Controls

You can create a control manually or automatically by downloading and importing UCF Authority Documents.

Creating Controls

To create a control, navigate to **GRC > Controls > All** and click **New**.

Control - Nightly security checks on manufacturing facilities.

Control ID

CTRL0002002

State

Active

Owning group

Field Services

Classification

Preventative

Owner

Keyna Bruni

Purpose

Process

Owner delegate

Genevieve Kekiwi

Control frequency

Continuous

Pertinent

☒

Compliance

0

Key control

☐

Non compliance

0

Name

Nightly security checks on manufacturing facilities.

Description

Evaluates effectiveness of nightly patrols by security guards in the manufacturering facilities.

Additional information

Update

Delete

Control Test Definitions (1)

Control Test Instances

Authority Documents

Citations

Policies

Risks

Other Versions

Control Test Definitions

New

Go to

Name

Search

1 to 1 of 1

Control = Nightly security checks on manufacturing facilities.

Run

On Demand

Ensure that the facility is secure

On Demand

Actions on selected rows...

1 to 1 of 1

Field	Description
Control ID	[Read-only] Unique identifier generated dynamically by the system.
Owning group	Group that owns the control.
Owner	User who owns the control.
Owner delegate	User who owns the control when the specified owner is unavailable.
Pertinent	Indicates that this control is relevant to your organization. By default, this check box is selected. Clear this check box if you do not plan to use this control and to prevent it from appearing in compliance reporting. Use this option to select appropriate controls from a large number of imported UCF controls. This field is available starting with the Fuji release.
Key control	Indicator that the control is considered key to preventing material risk, if selected.
State	Workflow field that determines the current state of the authoring process. Possible choices are: Draft , Active , and Inactive .
Classification	Control type being created. Possible choices are: Preventative , Corrective , and Detective .
Purpose	Approach that the control will take. Possible choices are: Process and Technical .
Control frequency	Basis for determining when the control is implemented. Possible choices are: Continuous , Event Driven , and Periodic .
Compliance	[Read-only] Percent of compliant control test instances associated with this control. This field is available starting with the Fuji release.
Non-compliance	[Read-only] Percent of non-compliant control test instances associated with this control. This field is available starting with the Fuji release.

Version	[Read-only] Version number for previous versions of this control. This value is a simple integer that is incremented by the system each time the control is updated. This field is hidden when the current version of the record is displayed. You can view all available versions by selecting records from the Other Versions related list. This field is available starting with the Fuji release.
Name	Descriptive name for this control.
Description	A long-form description of the control.
Additional information	Information of any type that is pertinent to this control. This field is available starting with the Fuji release.

Configure the form to show these fields

Authority document count	Total count of the authority documents that use this control. The purpose of this field is to calculate totals for the Super Control report.
Policy count	Total count of the policies that use this control. The purpose of this field is to calculate totals for the Super Control report.

Importing Controls from UCF

The United Compliance Framework (UCF) ^[1] provides authority documents containing controls that you can download into your instance and use in control test definitions. UCF provides quarterly updates that you can import into your system. By default, all UCF control documents are imported into GRC in an active state, ready for use. For more information about downloading and approving these documents, see UCF Authority Documents. Importing controls from UCF is available starting with the Fuji release.



Warning: Field values imported from UCF should be protected for data continuity and accuracy. *Do not* customize fields to allow UCF data to be edited. Use the **Additional information** field to display any additional details or specifications for this UCF entity that are unique to your organization, while preserving the original content from UCF.

Control - Do not send spam with hyperlinks to a country that has an anti-spam policy. Update Delete

Control ID

CTRL0002040

State

Active

Source

UCF

Classification

-- None --

Source Id

00284

Purpose

-- None --

Source Version

2014-08-25

Control frequency

-- None --

Owning group

Compliance

0

Owner

Non compliance

0

Owner delegate

Pertinent

☒

Key control

☐

Name

Do not send spam with hyperlinks to a country that has an anti-spam policy.

Description

Additional information

Update

Delete

Control Test Definitions (1)

Control Test Instances

Authority Documents (1)

Citations (1)

Policies

Risks

Other Versions

Control Test Definitions

New

Go to

Name

Search

1 to 1 of 1

Control = Do not send spam with hyperlinks to a country that has an anti-spam policy.

Anti-spam attestation

On Demand

Actions on selected rows...

1 to 1 of 1

Field	Description
Control ID	[Read-only] Unique identifier generated dynamically by the system.
Source	[Read-only] Source of the data in this control. UCF is the source of all controls imported from UCF authority documents. This field is available starting with the Fuji release
Source ID	[Read-only] Internal unique UCF identifier for this control. This field is available starting with the Fuji release.
Source version	[Read-only] Version of the UCF authority document that is the source file for this control. Previous versions of this control are listed in the Other versions related list. This field is available starting with the Fuji release.
Owning group	Group that owns the control.
Owner	User who owns the control.
Owner delegate	User who owns the control when the specified owner is unavailable.
Pertinent	Indicates if a UCF control is relevant to your organization. By default, this check box is selected and has a value of True . Clear this checkbox to mark this control as not pertinent to your organization and to prevent it from appearing in compliance reporting. This field is available starting with the Fuji release.
Key control	Indicator that the control is considered key to preventing material risk, if selected.
State	Workflow field that determines the current state of the authoring process. Possible choices are: Draft , Active , and Inactive .
Classification	Control type being created. Possible choices are: Preventative , Corrective , and Detective .
Purpose	Approach that the control will take. Possible choices are: Process and Technical .
Control frequency	Basis for determining when the control is implemented. Possible choices are: Continuous , Event Driven , and Periodic .
Compliance	[Read-only] Percent of compliant control test instances associated with this control. This field is available starting with the Fuji release.
Non-compliance	[Read-only] Percent of non-compliant control test instances associated with this control. This field is available starting with the Fuji release.
Version	[Read-only] Version number for previous versions of this control. This value is a simple integer that is incremented by the system each time the UCF control is updated. This number is not the same as the UCF Source version . The Version field is hidden when the current version of the record is displayed. You can view all available versions by selecting records from the Other Versions related list. For more information, see UCF Control Versions. This field is available starting with the Fuji release.
Name	[Read-only] Title of the control from the UCF document.
Description	[Read-only] Control from the UCF document. This is the actual content of the control.
Additional information	Information of any type that is pertinent to this control. This field is available starting with the Fuji release.

UCF Control Versions

The ServiceNow system creates a new version of a control each time a new UCF authority document is imported into GRC. When a new version of a control is created, the system adds the previous version to the **Other versions** related list in the Control form. These records are used for reference only and provide a history of each UCF control version's use. New control tests run against the current control version only. Only the latest version of each control appears in lists of controls.

Super Controls

A *super control* is a control shared by multiple authority documents. When a new UCF version of a super control is downloaded, the system links all authority documents using that control to the new version, even those authority documents not updated. This can result in unintended changes in the relationship between the shared control and any unmodified authority documents. Relationship changes can alter how compliance is evaluated for your organization. Be sure you know what affect these updated controls have on your audits. The system displays super controls in:

- UCF document details
- GRC update requests
- GRC update approval records
- Email notifications

UCF Documents

To view super controls in a UCF document, navigate to **GRC > Administration > Import UCF Content** and click a document card in the left column. The system lists all shared controls for that authority document in the top portion of the details pane.

16 CFR Part 310 Details

Published name	16 CFR Part 310, Telemarketing Sales Rule (TSR)
Type	Regulation or Statute
Category	North America
Released version	Q4 14 - Final
Release date	2003-01-01
Effective date	2003-01-29
Impact zones	Privacy protection for information and data Records management
URL	16 CFR Part 310

GRC super controls

Related to: [CobiT](#) by these controls:

- [Establish and maintain a data retention policy and data retention processes and determine how long to keep records and logs.](#)

Related to: [Australia CLERP](#) by these controls:

- [Establish and maintain a data retention policy and data retention processes and determine how long to keep records and logs.](#)

Related to: [10 CFR Part 73.54](#) by these controls:

- [Establish and maintain a data retention policy and data retention processes and determine how long to keep records and logs.](#)

GRC Update Requests

When you select UCF documents to import into GRC, the request for approval screen indicates if the selected documents contain super controls.

GRC Update Request for Approval

12 CFR Part 229 (updates GRC Super Controls)
16 CFR Part 310 Amendments

● Automatic approval is off, request will be sent for approval.

2 authority documents to request for approval.

SubmitClose

GRC Update Approvals

Users responsible for approving requests for UCF imports into GRC can see a list of super controls associated with an authority document in the Approval form.

< Approval

Update Approve Reject Delete

ApproverSystem Administrator

ApprovingGRC Update Status: 16 CF

StateRequested

Comments

Created byadmin

GRC Authority Documents16 CFR Part 310

UCF Authority Document16 CFR Part 310

Authority Document Source<http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&sid=bf60e7b87681ffc1030185f246d305&rgn=div5&view=text&node=16:1.0.1.3.34&idno=16>

GRC super controls

Related to: [CobIT](#) by these controls:

- Establish and maintain a data retention policy and data retention processes and determine how long to keep records and logs.

Related to: [12 CFR Part 229](#) by these controls:

- Establish and maintain a data retention policy and data retention processes and determine how long to keep records and logs.

Related to: [10 CFR Part 73.54](#) by these controls:

- Establish and maintain a data retention policy and data retention processes and determine how long to keep records and logs.

GRC Email Notification

When you import or update an authority document, an event called `control.versioned` triggers the **Common control update** email notification. By default, the system sends this notification to the GRC Executive Approver user and lists all super controls contained in the updated authority document.

Deleting Controls

You cannot delete a GRC record that has a linked dependency to another GRC record. The **Delete** button appears in records and record lists, but only *deactivates* the entity rather than removing it from the system. Deactivation clears the **Pertinent** check box in the record, which removes any links to other GRC entities. By default, deactivated records are filtered out of related lists. Manually created GRC records with no linked dependencies can be completely deleted from the system. UCF records imported into GRC tables can only be deactivated. Only users with the admin role can deactivate or delete GRC records.

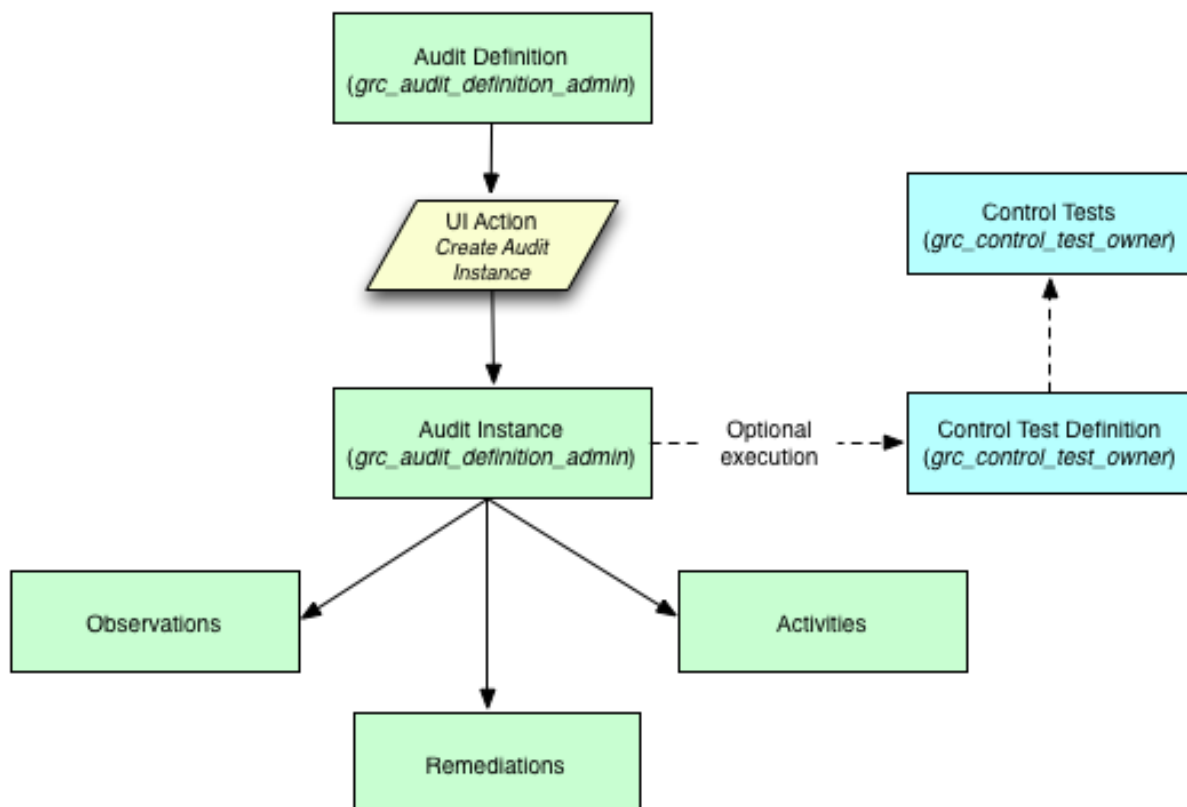
Managing Audits

Overview

Once policies are defined, put an audit process in place to verify that the policy, and any risk controls associated with it, are being followed.

Process Diagram

This diagram illustrates the process of managing an audit with Governance, Risk, and Compliance:



Creating an Audit Definition

The first step in the audit process is for the auditor to create the necessary audit.

To create an audit definition, navigate to **GRC > Administration > Audit Definitions** and click **New**. Populate the following fields from the table.

< Audit Definition

ID

AUD0002001

State

Current

Name

Building access security

Execution group

Owning group

Owner

Alfonso Griglen

Short description

Building access security practices

Description

Determine if proper procedures are being followed by security personnel during building access checks.

Submit

Field	Input Value
ID	A unique ID for the audit definition, populated by number maintenance.
Name	A name for the audit definition.
Owning group	A reference to a group to have ownership over the audit process.
Owner	A reference to a user to have ownership over the audit process.
State	Where in the drafting process the definition is.
Execution group	A reference to the group that will execute the audit.
Short Description	A short description of the audit.
Description	A full description of the audit.

The related list **Control Test Definitions** can be used to specify control tests to perform during the audit. Use the **Scope** related list to define specific locations or business units to which the audit applies.

Audit Requirements in Versions Prior to Fuji

Audit requirements can be defined to create a relationship between the audit and authoritative source content, allowing auditors to determine whether the audit is in compliance with particular sections of regulation or policy. Requirements were removed from the Audit Definition form starting with the Fuji release, and the requirements functionality was replaced by the use of citations.

To define audit requirements:

1. Navigate to **GRC > Audit Definitions**.
 2. Click **Edit** in the **Requirements** related list and add citations.
 3. After you add the audit requirements to the list, click **Edit** in the **Control Test Definitions** related list and add a definition to associate with the control test.
- After the audit requirements are associated with the audit definition, these requirements create Requirements records associated to each audit instance generated. The Requirements form has the following fields:

Field	Input Value
Number	A number identifier for the requirement, populated by number maintenance.
Requirement	A reference to the citation which contains the original source of this requirement.
Name	The Name field from the citation record.
Type	The Type field from the citation record.
Authority document	The Authority Document field from the Citation record.
Control test definition	The control test associated with the requirement.
Supporting control test	The control test instance whose results are either compliant or not compliant with this requirement.
Compliant	A checkbox to record whether the audited subject is compliant with this requirement.
State	The state field from task.
Assignment group	A group assigned to assess the requirements.
Assigned to	A user assigned to assess the requirements.

Creating an Audit Instance

Once the audit is defined, click **Create Audit Instance** under **Related Links** to generate an Audit Instance record, which manages the audit process. The audit definition must be in the **Current** state for this control to appear. The audit is automatically assigned to the owning group, and the event `grc_audit.inserted` is recorded in the event log by the business rule **planned task global events**. By default, any *active* control test definitions associated with the audit definition are executed and create control test instances when the audit instance is created.

Audit Definition - Building access security

ID: AUD0002001 State: Current

Name: Building access security Execution group: [Search]

Owing group: [Search] Owner: Alfonso Griglen [Search]

Short description: Building access security practices

Description: Determine if proper procedures are being followed by security personnel during building access checks.

Update Delete

Related Links

[Create Audit Instance](#) Click to execute the control test definition

Control Test Definitions New Edit... Go to: Control test definition Search

1 to 1 of 1

Audit definition = Building access security

Control test definition	Control	State
Ensure all entrances to buildings in San Deigo are pass card enabled	All buildings fitted with electronic sec...	Active

1 to 1 of 1

Recording Audit Observations

The observations related list on the Audit Instance record can be used to record any information uncovered in the audit process. Remediation tasks can be generated directly from audit observations. For instance, the audit observation **There is no process around off-boarding** can lead to the remediation task **Define off-boarding process**.

Using the Related Items tool from the Many to Many Task Relations Plugin, relate audit observations to any task on the platform by explicitly defined relationships.

Recording Audit Activities

Audit Activities are used to record and track the tasks required to perform an audit instance. To create an Audit Activity, navigate to the appropriate audit instance and use the **Audit Activities** related list.

Populate the following fields:

Field	Input Value
Number	An incremented identifier for the audit activity, generated using Managing Record Numbering.
Requested By	A reference to the user who requested the audit activity.
Requestor Reference	A reference to a record in a third party system where the requestor may be tracking the requirement
Opened By	A reference to the user who created the audit activity.
Opened	A date-time stamp for when the audit activity was created.
State	A choice list for status of the task: <ul style="list-style-type: none">• Pending• Open• Work in Progress• Closed Complete• Closed Incomplete• Closed Skipped
Assignment Group	A reference to the group assigned to perform the audit activity.
Assigned To	A reference to the user assigned to perform the audit activity.
Closed	A date-time stamp for when the audit activity was closed.
Closed by	A reference to the user who closed the record.
Short Description	A short description of the audit activity.
Description	A more detailed description of the audit activity.
Work Notes	A journal field for recording work performed on the audit activity.

Article Sources and Contributors

Governance, Risk and Compliance	<i>Source:</i> http://wiki.servicenow.com/index.php?oldid=241015	<i>Contributors:</i> Fuji.publishing.user, Renee.Phillips, Stacey.schwingle, Steven.wood
Defining Authoritative Sources	<i>Source:</i> http://wiki.servicenow.com/index.php?oldid=243290	<i>Contributors:</i> Fuji.publishing.user, Parmeet.singh, Stacey.schwingle
Managing Policies	<i>Source:</i> http://wiki.servicenow.com/index.php?oldid=243291	<i>Contributors:</i> Fuji.publishing.user, Phillip.salzman, Stacey.schwingle, Steven.wood
Defining Risks	<i>Source:</i> http://wiki.servicenow.com/index.php?oldid=243292	<i>Contributors:</i> Fuji.publishing.user, Phillip.salzman, Stacey.schwingle, Steven.wood
Managing Controls and Tests	<i>Source:</i> http://wiki.servicenow.com/index.php?oldid=243293	<i>Contributors:</i> Fuji.publishing.user, Stacey.schwingle, Steven.wood
Managing Audits	<i>Source:</i> http://wiki.servicenow.com/index.php?oldid=243294	<i>Contributors:</i> Fuji.publishing.user, Phillip.salzman, Stacey.schwingle, Steven.wood

Image Sources, Licenses and Contributors

Image:Warning.gif *Source:* <http://wiki.servicenow.com/index.php?title=File:Warning.gif> *License:* unknown *Contributors:* CapaJC

Image:GRC_Nav_Menu.png *Source:* http://wiki.servicenow.com/index.php?title=File:GRC_Nav_Menu.png *License:* unknown *Contributors:* Fuji.publishing.user

File:GRC_New_Auth_Source.png *Source:* http://wiki.servicenow.com/index.php?title=File:GRC_New_Auth_Source.png *License:* unknown *Contributors:* Fuji.publishing.user, Steven.wood

Image:Caution-diamond.png *Source:* <http://wiki.servicenow.com/index.php?title=File:Caution-diamond.png> *License:* unknown *Contributors:* John.roberts, Publishing.user

File:GRC_Sample_UCF_Auth_Src.png *Source:* http://wiki.servicenow.com/index.php?title=File:GRC_Sample_UCF_Auth_Src.png *License:* unknown *Contributors:* Fuji.publishing.user, Steven.wood

File:GRC_Policy.png *Source:* http://wiki.servicenow.com/index.php?title=File:GRC_Policy.png *License:* unknown *Contributors:* Fuji.publishing.user

Image:GRC-criteria.png *Source:* <http://wiki.servicenow.com/index.php?title=File:GRC-criteria.png> *License:* unknown *Contributors:* Fuji.publishing.user, Guy.yedwab

File:GRC-criteria2.png *Source:* <http://wiki.servicenow.com/index.php?title=File:GRC-criteria2.png> *License:* unknown *Contributors:* Fuji.publishing.user

Image:GRC-criteria-Eureka.png *Source:* <http://wiki.servicenow.com/index.php?title=File:GRC-criteria-Eureka.png> *License:* unknown *Contributors:* Fuji.publishing.user

File:GRC-criteria_early.png *Source:* http://wiki.servicenow.com/index.php?title=File:GRC-criteria_early.png *License:* unknown *Contributors:* Fuji.publishing.user

File:GRC_Control_Process_Diagram.png *Source:* http://wiki.servicenow.com/index.php?title=File:GRC_Control_Process_Diagram.png *License:* unknown *Contributors:* Steven.wood

File:IT_GRC_Control.png *Source:* http://wiki.servicenow.com/index.php?title=File:IT_GRC_Control.png *License:* unknown *Contributors:* Fuji.publishing.user, Steven.wood

File:GRC_UCF_Control.png *Source:* http://wiki.servicenow.com/index.php?title=File:GRC_UCF_Control.png *License:* unknown *Contributors:* Fuji.publishing.user, Steven.wood

File:Super_Controls_UCF_Details.png *Source:* http://wiki.servicenow.com/index.php?title=File:Super_Controls_UCF_Details.png *License:* unknown *Contributors:* Fuji.publishing.user

File:Super_Controls_Request.png *Source:* http://wiki.servicenow.com/index.php?title=File:Super_Controls_Request.png *License:* unknown *Contributors:* Fuji.publishing.user

File:Super_Controls_Approval.png *Source:* http://wiki.servicenow.com/index.php?title=File:Super_Controls_Approval.png *License:* unknown *Contributors:* Fuji.publishing.user

File:GRC_Audit_Process_Diagram.png *Source:* http://wiki.servicenow.com/index.php?title=File:GRC_Audit_Process_Diagram.png *License:* unknown *Contributors:* Fuji.publishing.user

File:GRC_Audit_Definition.png *Source:* http://wiki.servicenow.com/index.php?title=File:GRC_Audit_Definition.png *License:* unknown *Contributors:* Fuji.publishing.user

File:GRC_Execute_CTD_from_Audit.png *Source:* http://wiki.servicenow.com/index.php?title=File:GRC_Execute_CTD_from_Audit.png *License:* unknown *Contributors:* Fuji.publishing.user