knowledge17

May 7–11, 2017 • Orange County Convention Center • Orlando, FL

Lab Guide

How ServiceNow Can Help Your Compliance Journey to GDPR

Manoj Patel & Eric Le Martret

Default Login / Password: knowledge17

Lab Sponsored by Microsoft Azure

Microsoft

servicenow

This
Page
Intentionally
Left
Blank

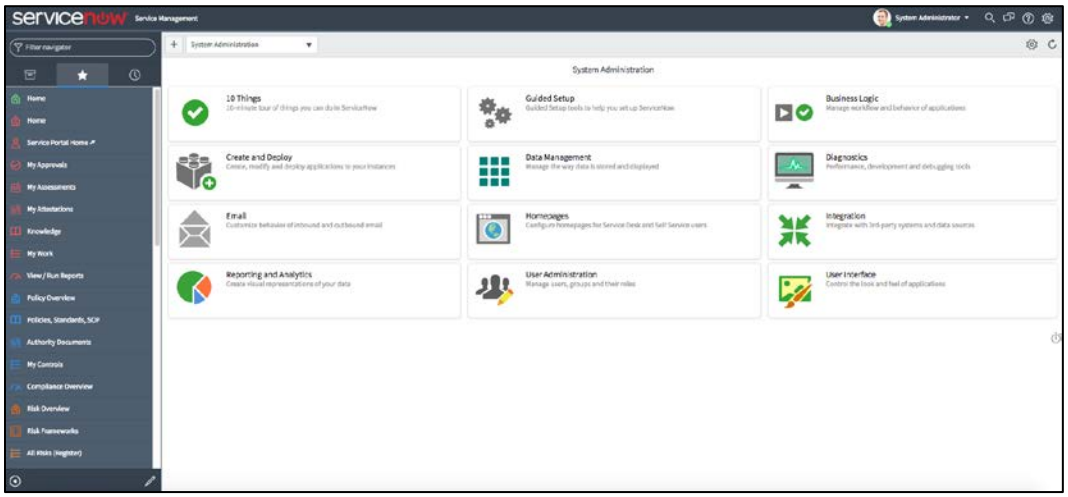
Lab Goal

The goal of this lab is to understand GDPR (General Data Protection Regulation) requirements, its impact on your organization, and how ServiceNow can help your compliance journey to GDPR. ServiceNow Governance, Risk, and Compliance (GRC) helps bring order to an enterprise's compliance requirements to GDPR. It provides best practices to meet the GDPR requirements. This lab explains key ServiceNow application to support GDPR and names the key citations (regulatory requirements) for GDPR.

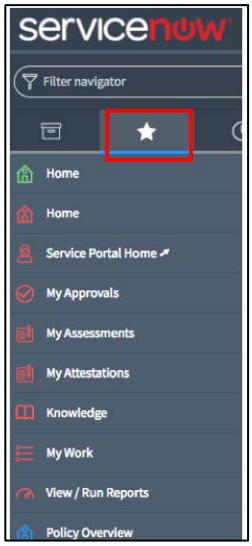
Lab 1.0
Apps & Dashboard

Getting Started – Log on to Your Training Instance

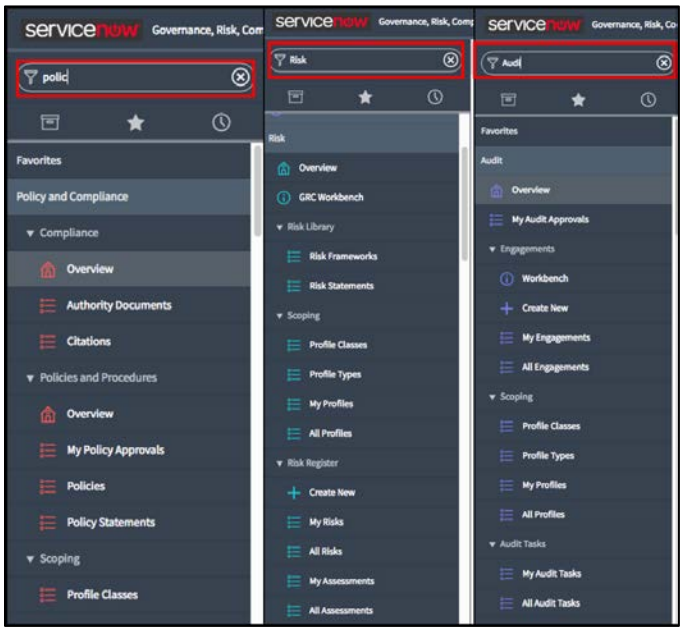
1. Navigate to the unique instance URL provided to you.
2. Log on with the provided credentials.
3. See your homepage.



4. See your favorite applications by clicking on the **star (★)** next to the application.



5. Discover GRC applications and its modules by typing first few letters of **Policy & Compliance**; **Risk Management & Audit Management**.

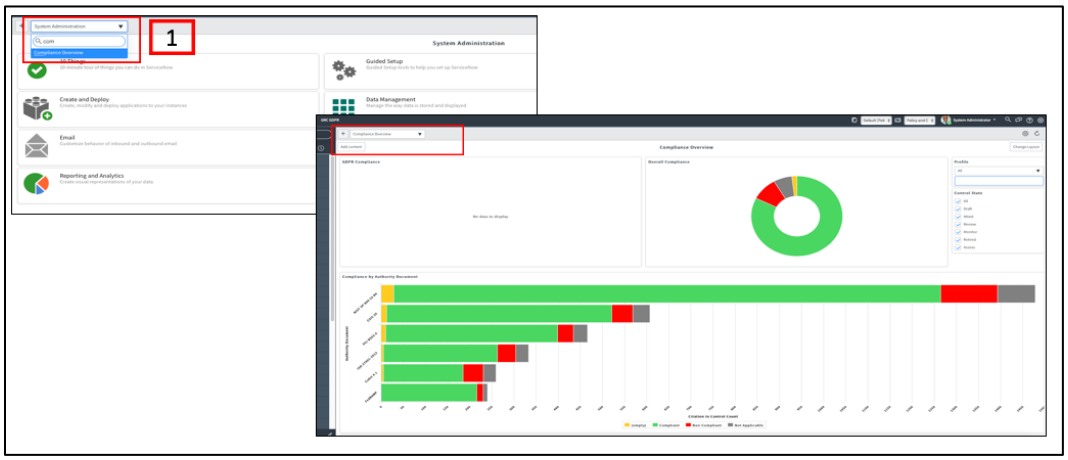


Check Your Homepage

1. Click the **ServiceNow** logo.



2. In the homepage window, search for compliance from the drop-down list.



3. Select **Compliance Overview**.

4. See initial Compliance status. You should see **GDPR Compliance** report as empty for now. The related **gauges/reports** are updated as you progress with the lab.

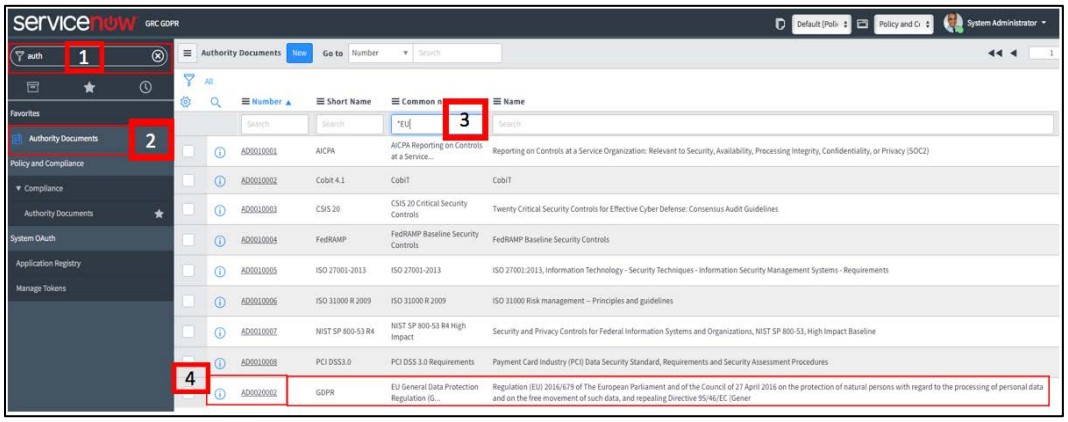
Lab Goal

This lab explores the GDPR authority document. It also explains the different citations for regulatory requirements.

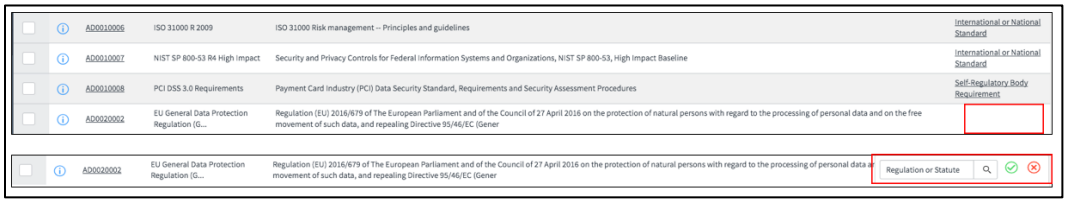
Lab 1.1 Authority Document GDPR

GDPR Authority Document

1. Type **authority** in **Filter Navigator** to search Authority Documents.
2. Click **Authority Documents.**
3. Search ***EU** under **Authority Documents** in the **Common Name** field.



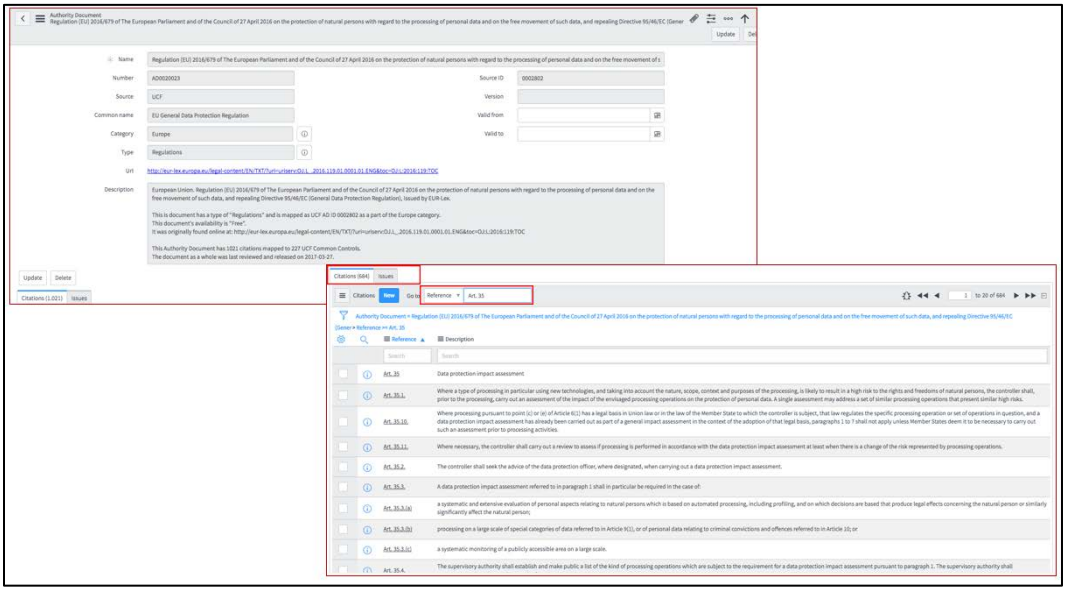
Note: See example below. If your **Type** field for **EU GDPR** Authority Document is empty, you can add the relevant type by double clicking on the empty field.



4. Click the **EU General Data Protection link (begins with AD00)**. (You might have different authority document number.)
5. See overall **GDPR** information.
6. Scroll to **related lists** and click on the **Citations**.

7. Search for **Art. 35** in **Reference** field**.**

8. See relevant article, information and respective subsections.



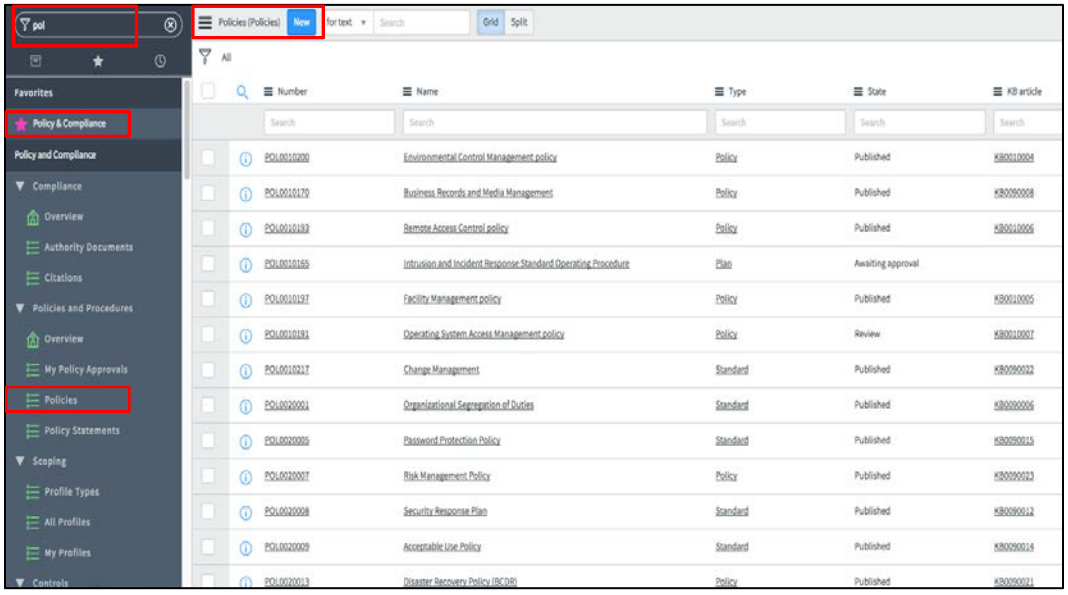
Lab Goal

This lab explains how to create an organizational policy and policy statements that matches requirements and describes outlines for GDPR.

Lab 2.0 Policy Creation

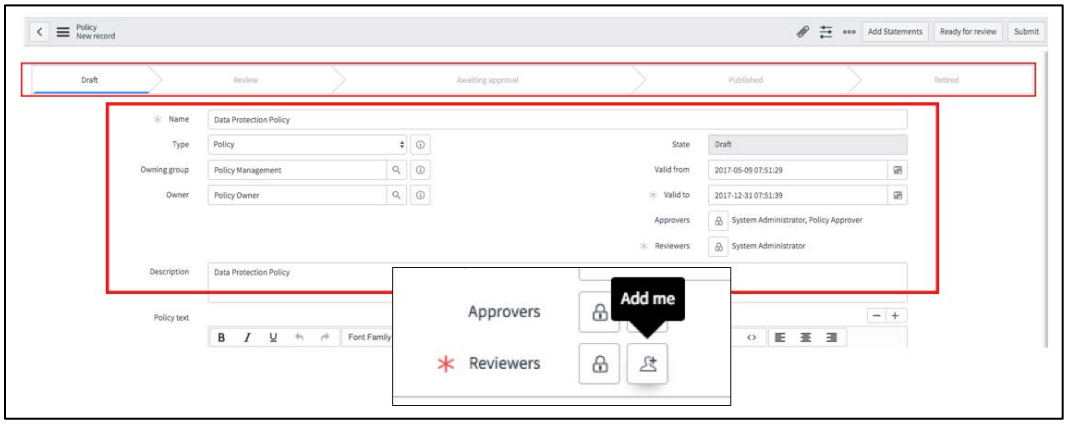
Policy Creation

1. Go to **Policy & Management** application.
2. Look for **Policies**. Click **Policies** to list them.
3. Click **New** at the top of the policies page.



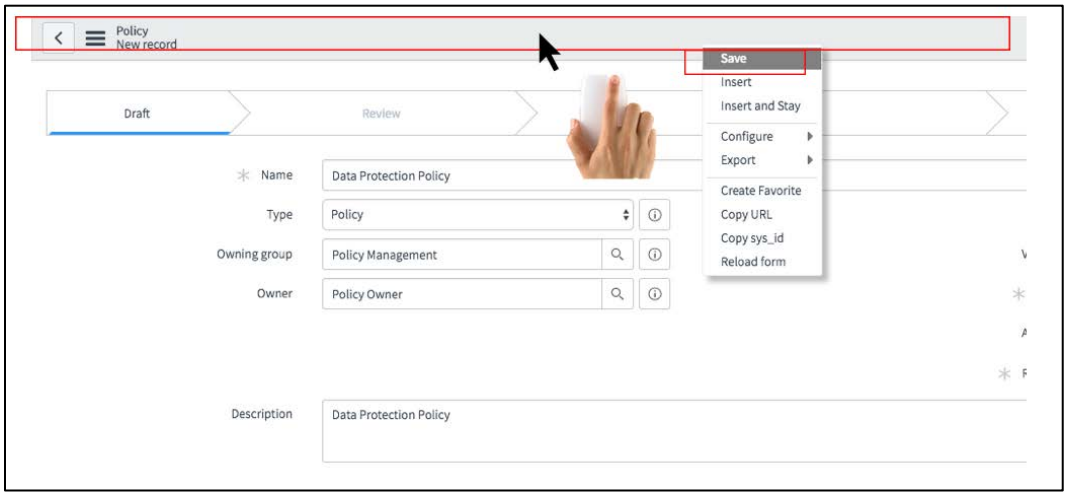
4. You see a full **Policy Life Cycle Stages** listed on the top of the record.

5. Fill out **New Policy Record** as shown. You can click on  icon to add yourself (**System Administrator**) or click on the lock icon to add **Policy Approver**.



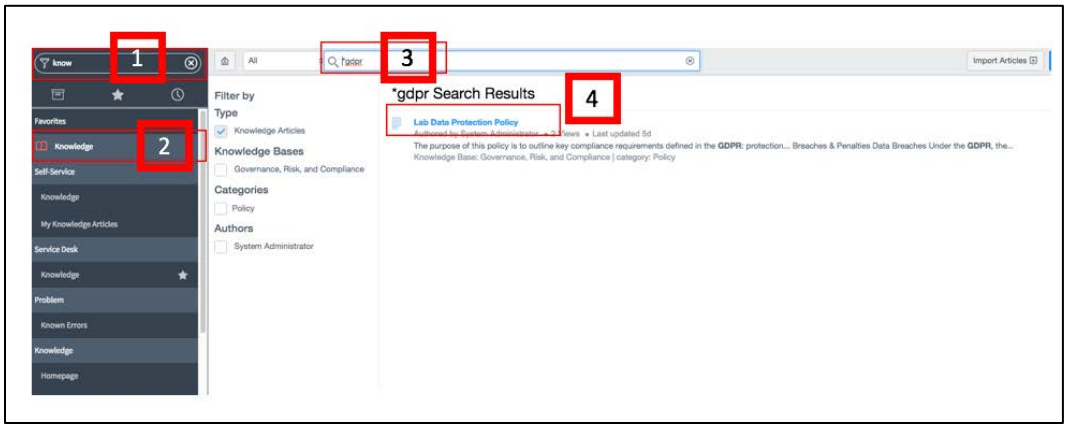
Note: You can provide any valid dates for this lab purpose. We have skipped any additional Policy Reviewer step here for simplicity.

6. To save the record, right-click on the **Policy Record bar**, open the drop-down menu, and click **Save**.



7. Type **Knowledge** in Filter Navigator.

8. Click **Knowledge** application.

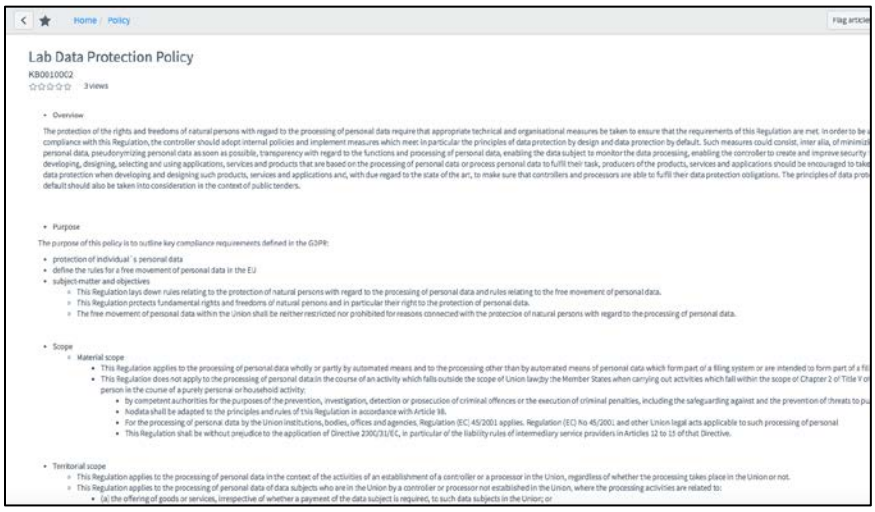


9. Search for ***gdpr** in the search bar.

10. You see a Lab Data Protection Policy.

11. Open the **Policy**.

12. The **Lab Data Protection policy** describes different sections required for a Data Protection policy. Pl. review the policy content.



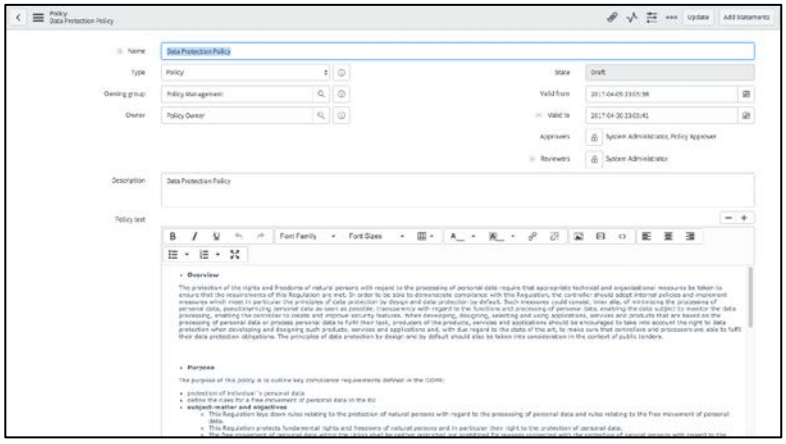
13. Copy content of the Lab Data Protection Policy.

14. Return to your policy by clicking on the history (**)**icon. Click the **Policy** you just created. You should be now back in the Policy Record.



15. Paste the copied content into **Policy Text** field.

16. **Save** the record. (as in step #6).

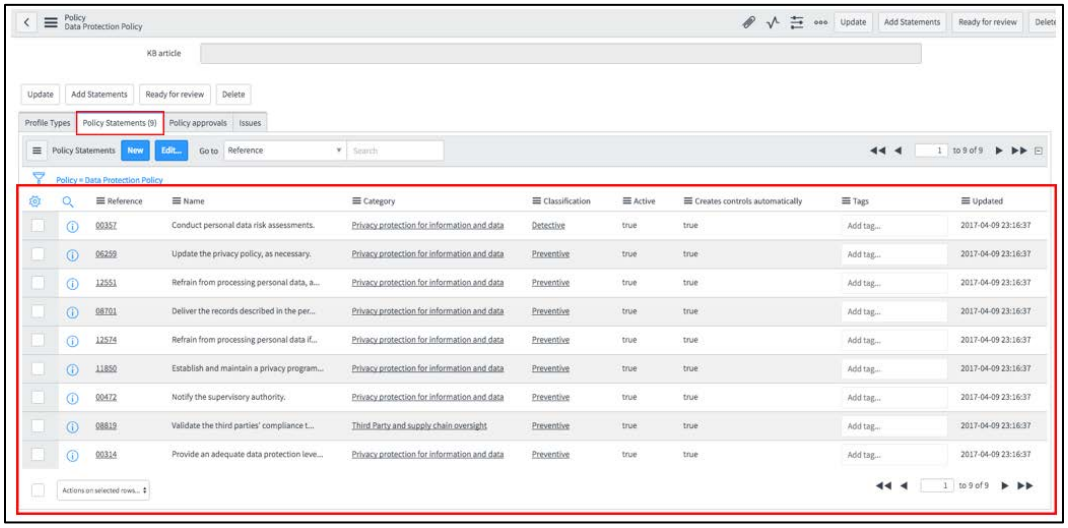


Now assign relevant Policy Statements to the Policy.

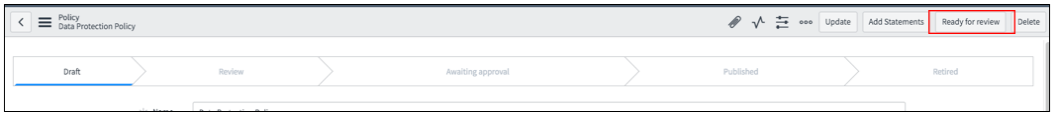
1. Generate Policy Statements that are defined for the policy by clicking **Add Statements**.



2. Scroll to related lists and click on **Policy Statements.** You see 9 policy statements added to the Policy.

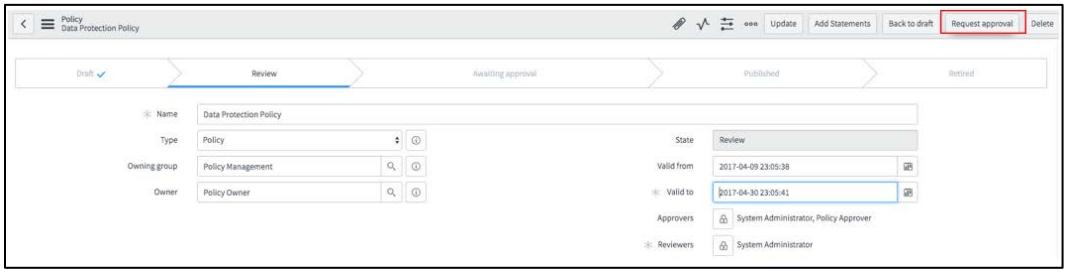


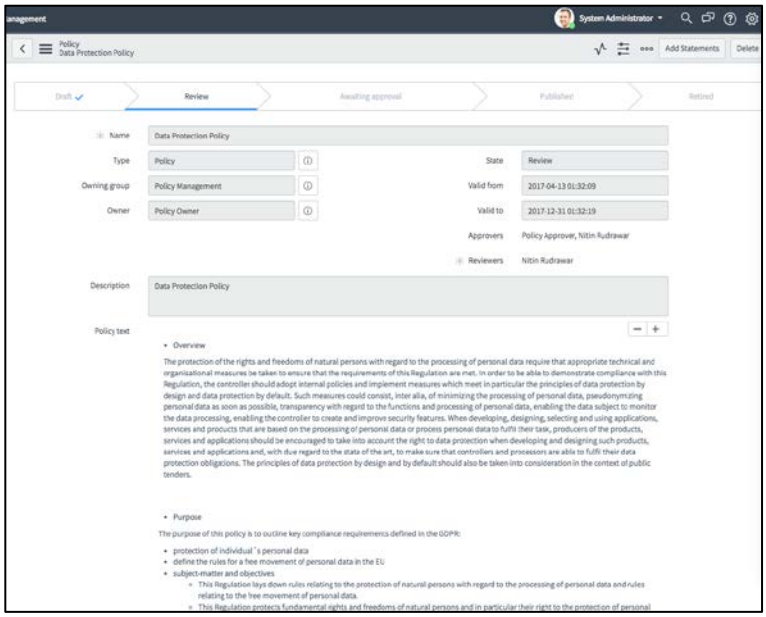
3. Move forward into Policy Life Cycle. Go to next stage and click **Ready for Review**.



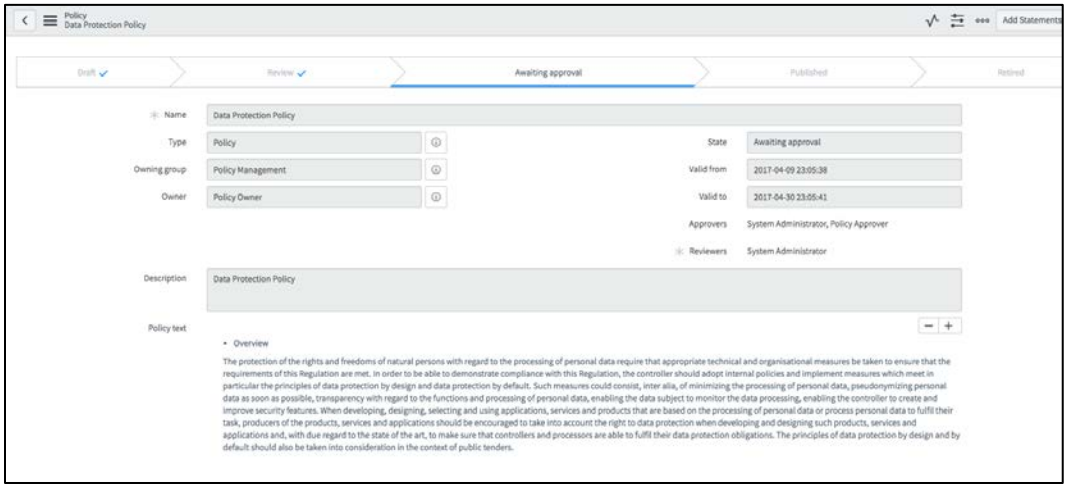
The policy moves to next stage **Review** in the Life Cycle Flow. A reviewer can now review the Policy. For this lab go directly to next step: **Approval**.

1. Click **Request Approval**. Approval request goes to **Policy Approver** & **System Administrator.** The policy form field becomes now read-only as shown below in 2nd example.





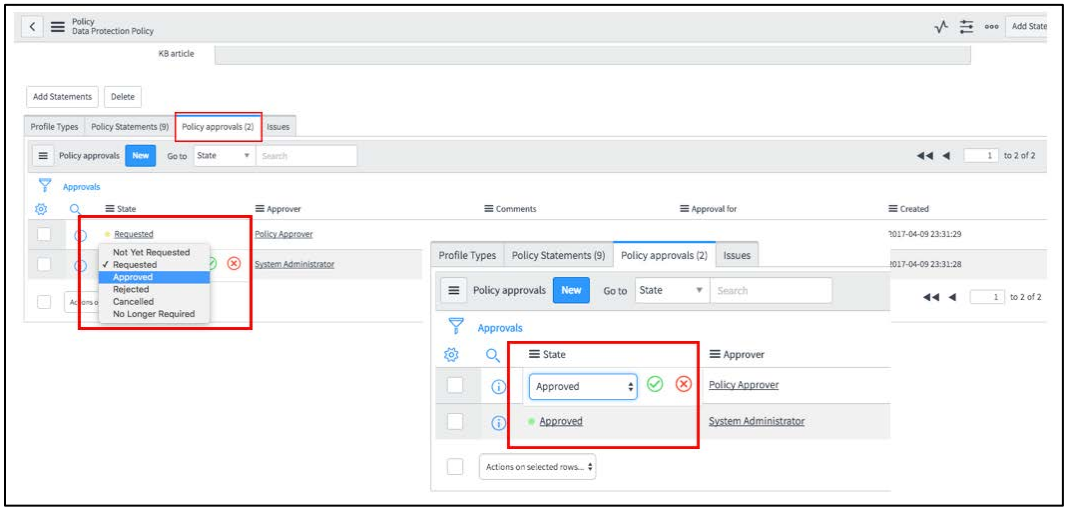
2. After requesting approval, policy life cycle state changes to **Awaiting approval** as shown below.



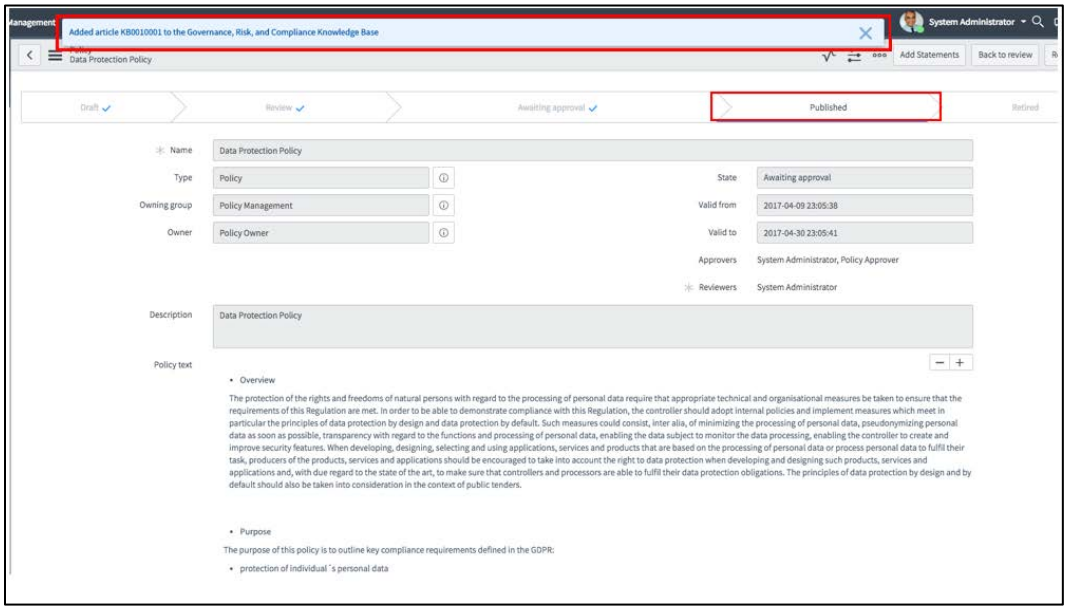
3. Scroll to related lists and click **Policy Approvals**.



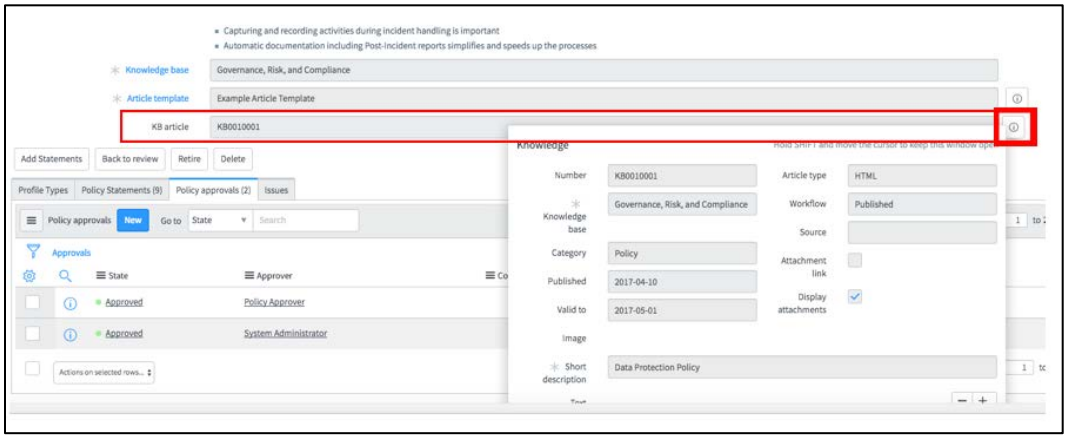
4. There are two records waiting for approvals. Double-click next to **Requested** (at the end of the word) and select **Approved** for each approver.



5. Reload form. The Policy Record has moved to state **Published**. Also, a Knowledge Article has been published.



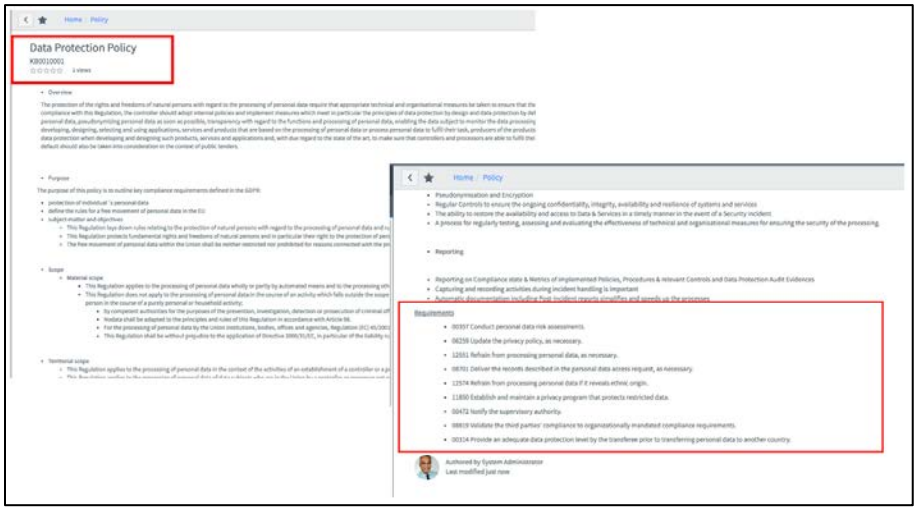
6. Scroll to **KB Article** and click the information icon at the end of the line.



7. A Knowledge record window opens. Scroll to **View Article** under **Related links** in this record.

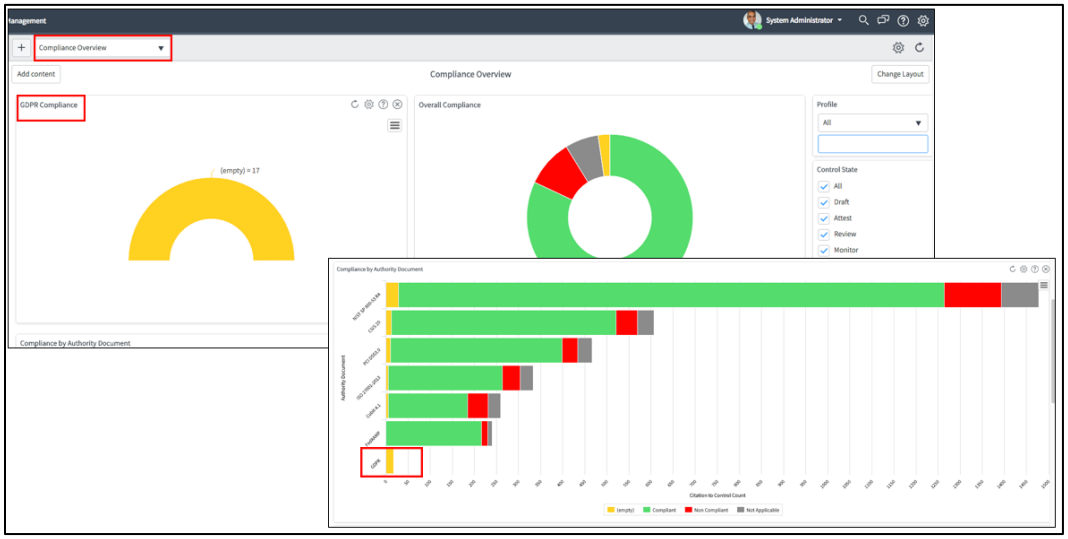
8. Click **View Article**.

9. See the KB-Article that has been created automatically with related requirements listed at the bottom of the article.



You completed a full Policy Life Cycle.

1. Return to the Dashboard and check **Compliance Overview**. The **GDPR Compliance** gauge is created and in empty status.



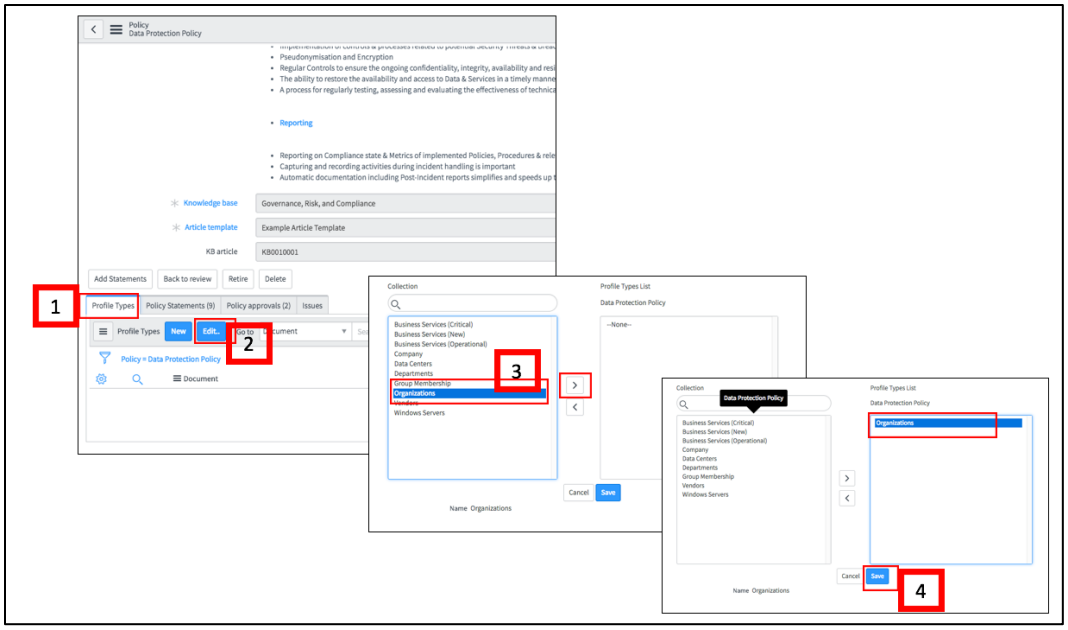
Lab Goal

This lab explains how to create Profile Type and assign Risk Framework to assess compliance requirements for a Profile. A profile – *An entity we need to check for compliance requirements* — will have then associated policy and policy statements you just created. You add risks to the Profile Type and see what could be potential impact of noncompliance to a Profile.

Lab 2.1
Profile Type, Profile & Risks

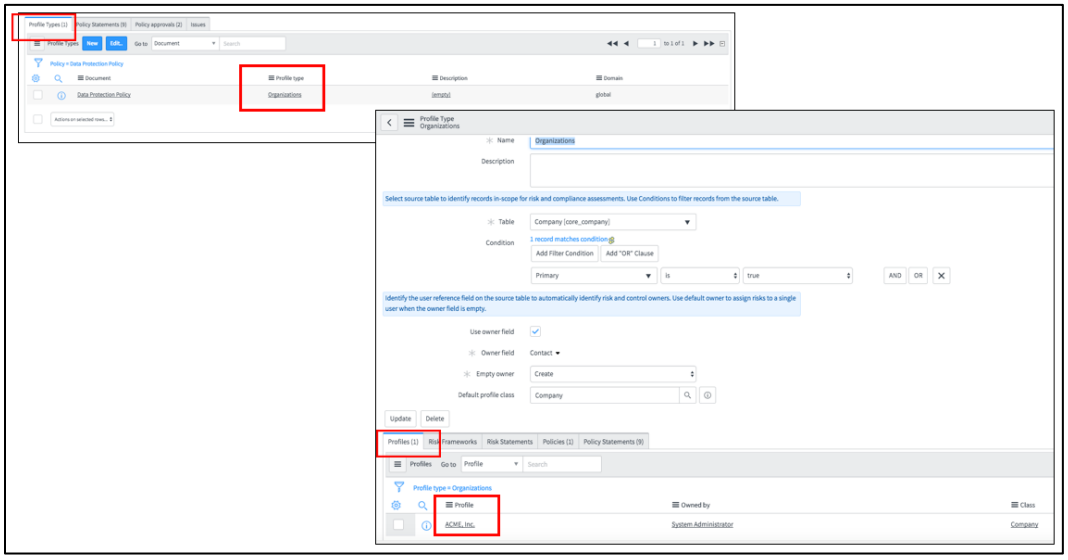
Profile Type, Profile & Risk Framework

1. Return to the Policy Record by clicking on history icon. (as in Lab 2.0)
2. Scroll to related lists and click **Profile Type** in the Policy record.
3. Click **Edit** under **Profile Type**.



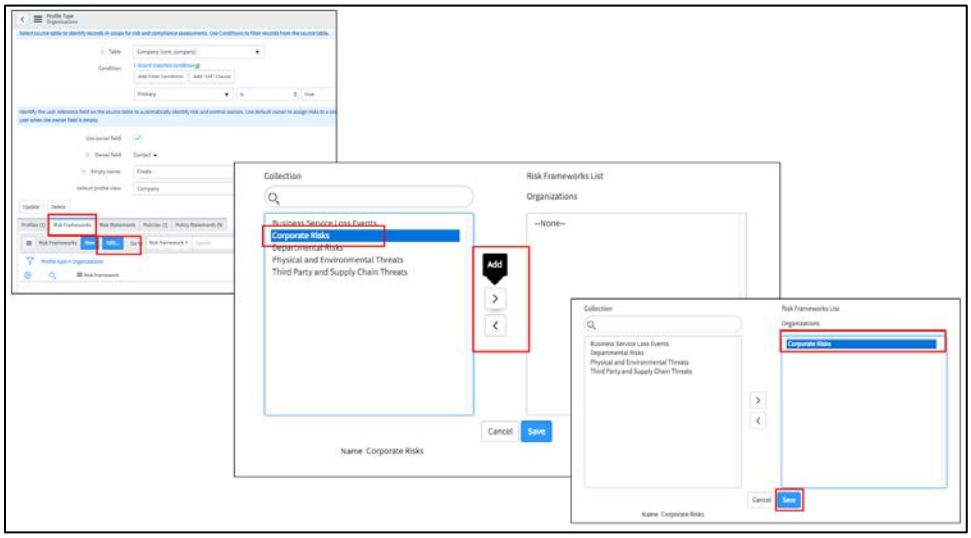
4. Click **Organizations**, move it into right window, and click **Save.**
5. You return to the Policy record. Scroll down and click on **Organizations** under **Profile Type** related list.

6. **Profile Type** record opens in a new window. A **Profile**, **ACME Inc.**, is assigned to this Profile Type.

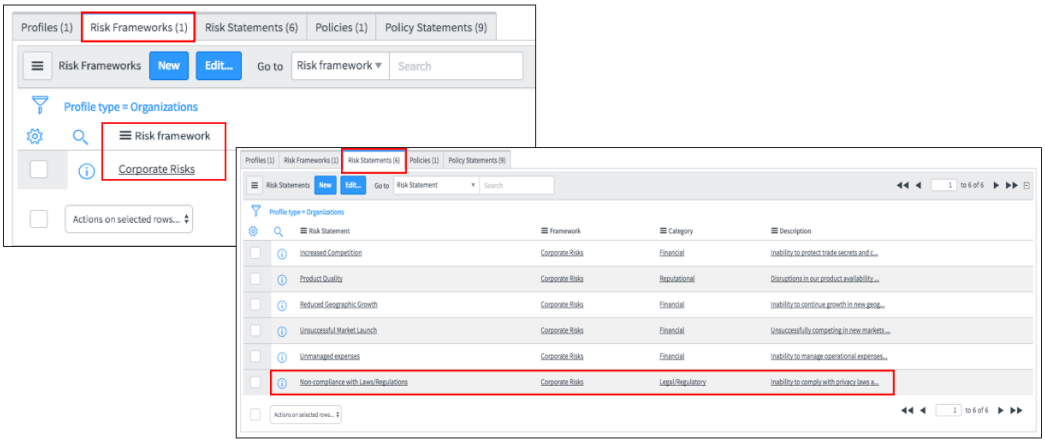


7. **Policies** & **Policy Statements** appear in the related list, created in earlier steps.

8. Now, add **Risk Framework** to the **Profile Type** as shown below. Add **Corporate Risks** to Profile type and click **Save**.



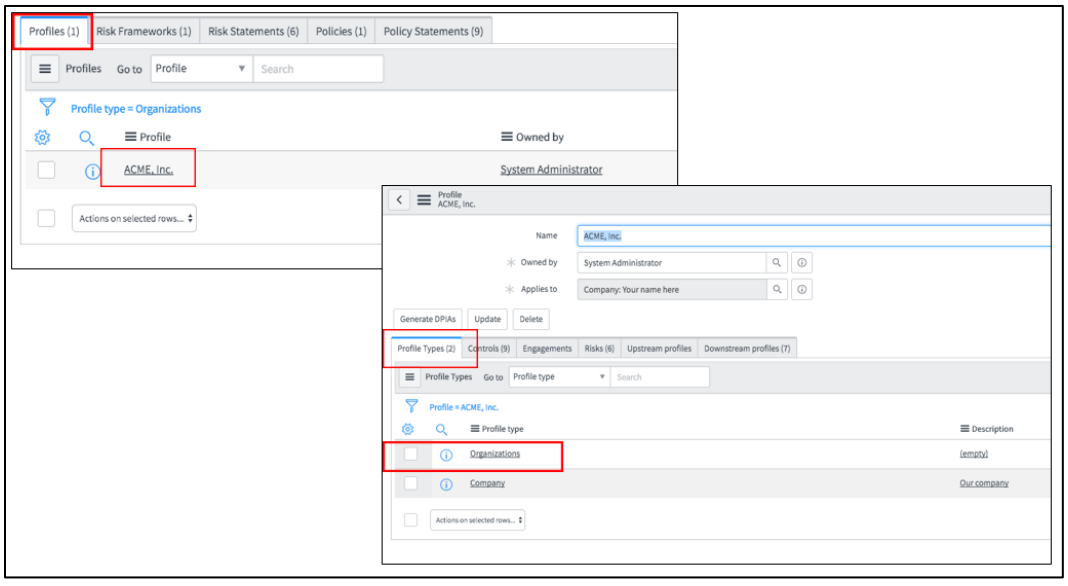
9. The **Risk Framework** is now assigned to **Profile Type** and **Risk Statements** are automatically added to that **Profile Type**. Reload the form.



10. Click on **Risk Statements** to see assigned **Risk Statements**.

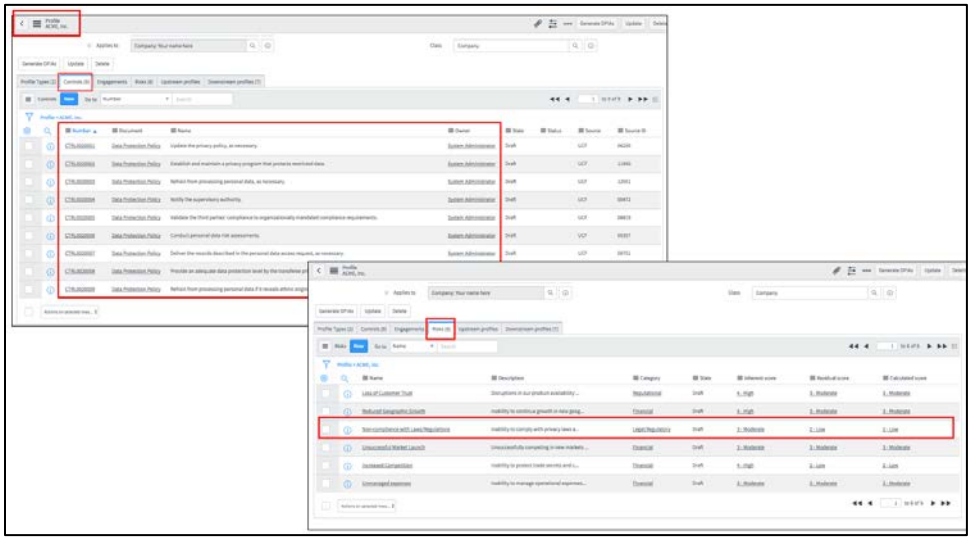
11. You should have some **Risk Statements**, including **Non-compliance with Law/ Regulations.** You revisit this **Risk Statement** later**.**

12. Return to **Profile** under Related lists. Click on Profile **ACME Inc**.



13. The Profile window contains **Organizations** in the **Profile Type** related list.

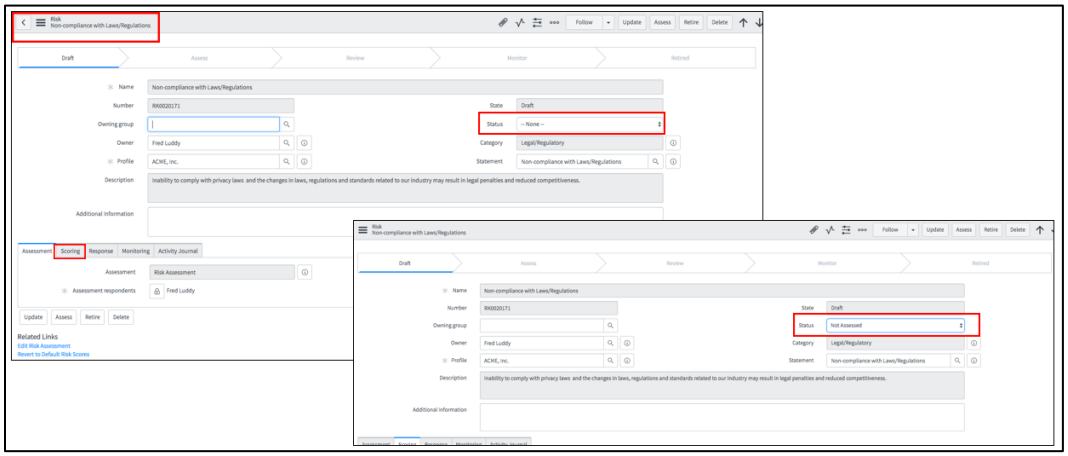
14. Click the **Controls** tab, next to **Profile Type**. There are 9 controls allocated to this **Profile** as requirements described in the Policy.



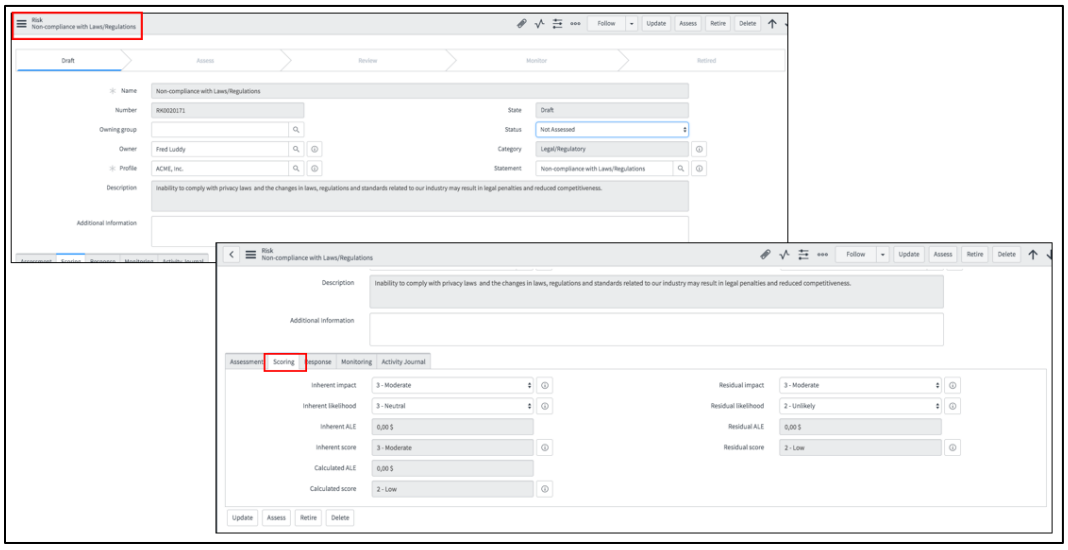
15. Click **Risks** to see the assigned Risks.

16. Click **Non-compliance with Law/ Regulations** risk. Now you are in **Risk** Record.

17. Change the Risk Life Cycle status in the form from **none** to **Not Assessed.**



18. Review all the fields in this risk record. Scroll down and click on **Scoring** tab. You should have all initial quantitative values at zero, since you have not assigned or tested controls related to this risk.



19. Change the **Scoring** record for **Inherent and Residual impact & Likelihood** as following:



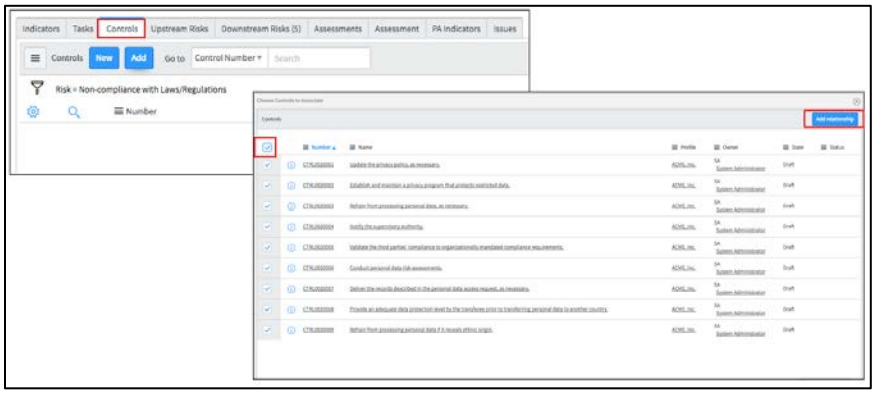
20. **Save** the record. **Reload** the risk record form to see new values.

Add controls to associate GDPR requirements to the risk.

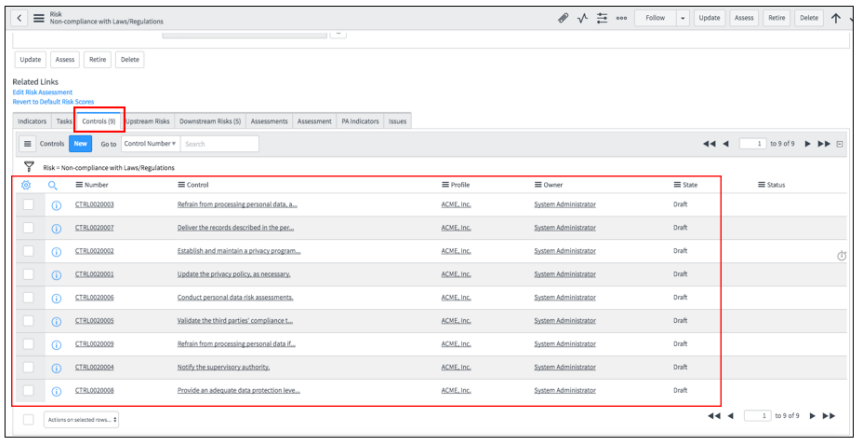
1. Scroll down and go to related lists. Click on **Controls**. Click on **Add**.

2. A new window opens to choose controls to associate them with the risk.

3. Select All controls and click **Add Relationship**.



4. There are 9 controls associated to that risk.



5. After adding these controls, save the record. The risk score remains the same since you have not yet executed controls.

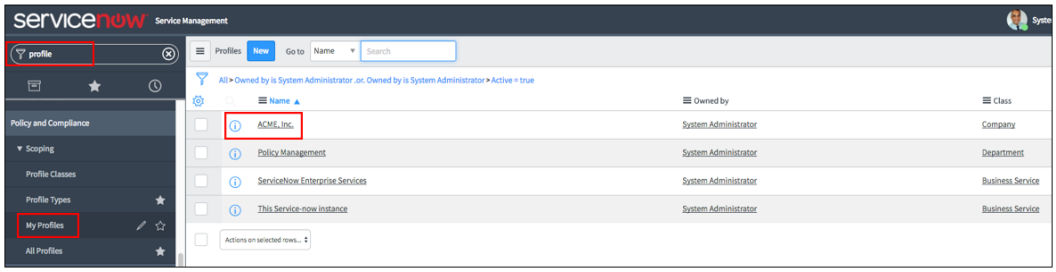


Lab Goal

This lab explains how to generate attestations for Data Protection requirements described in the Policy for the ACME Inc. Depending on attestations responses, controls status changes from draft to compliant or noncompliant and has an effect on risk scoring.

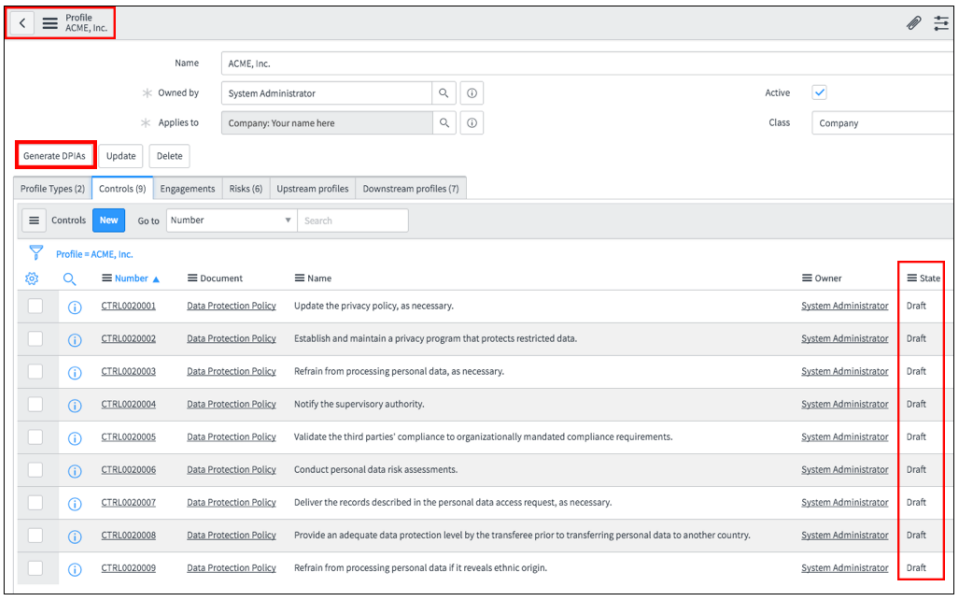
Lab 3.0
Attestations

1. Return to your **Profile**.

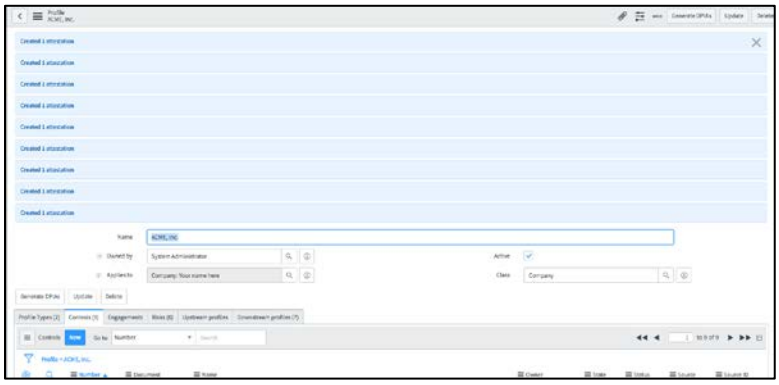


2. Click **ACME Inc.**

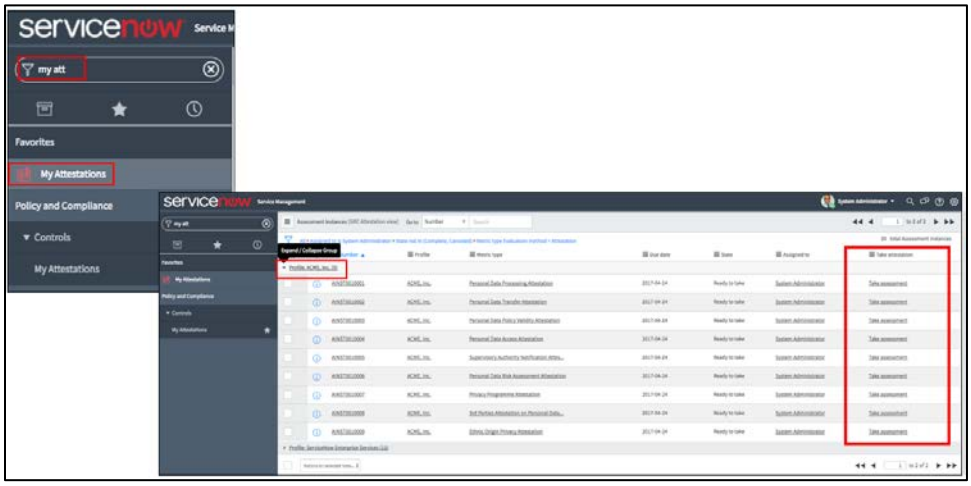
3. Click **Generate DPIAs** (Data Protection Impact Assessments).



4. There are 9 created **attestations**.

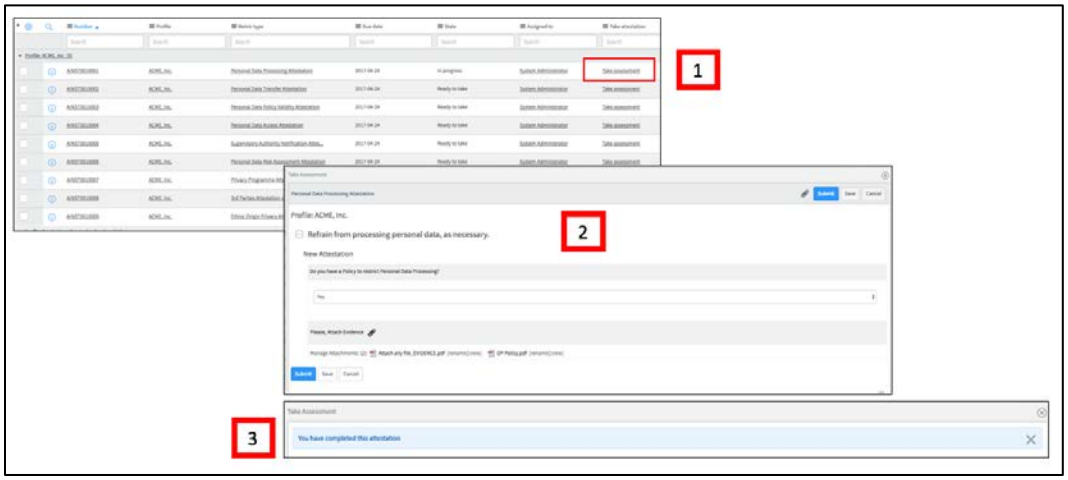


5. Search in filter navigator for **My Attestations** and click it.

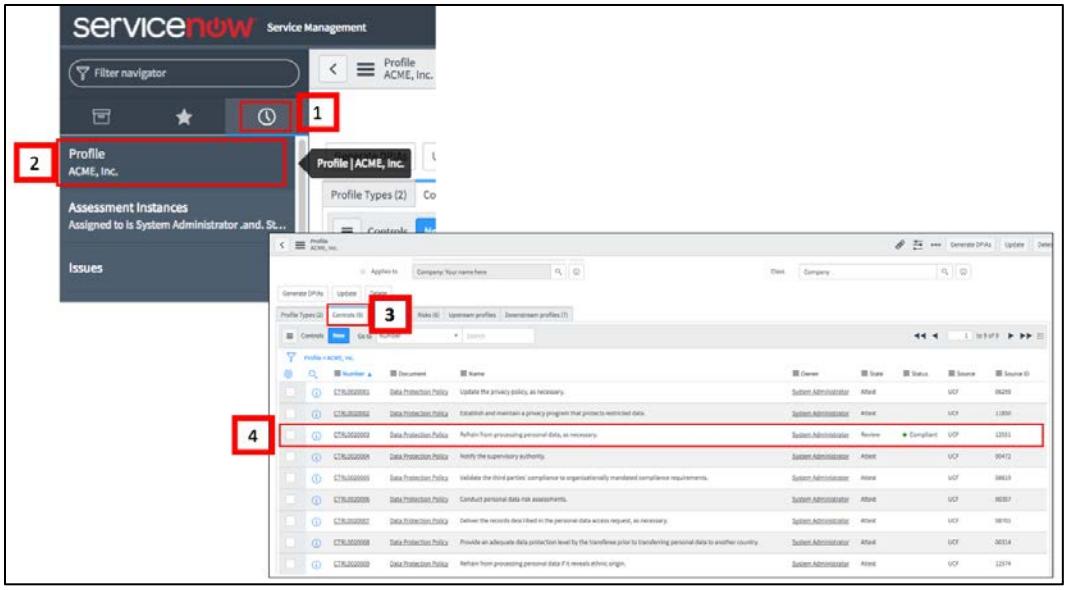


6. Expand the **Profile ACME Inc**. to see full record. You should have now 9 attestations in **Ready to Take** state.

7. Take one **attestation** and submit it. If asked to attach evidence, attach any (small size) file from your laptop. You can also provide multiple attachments for the evidence.

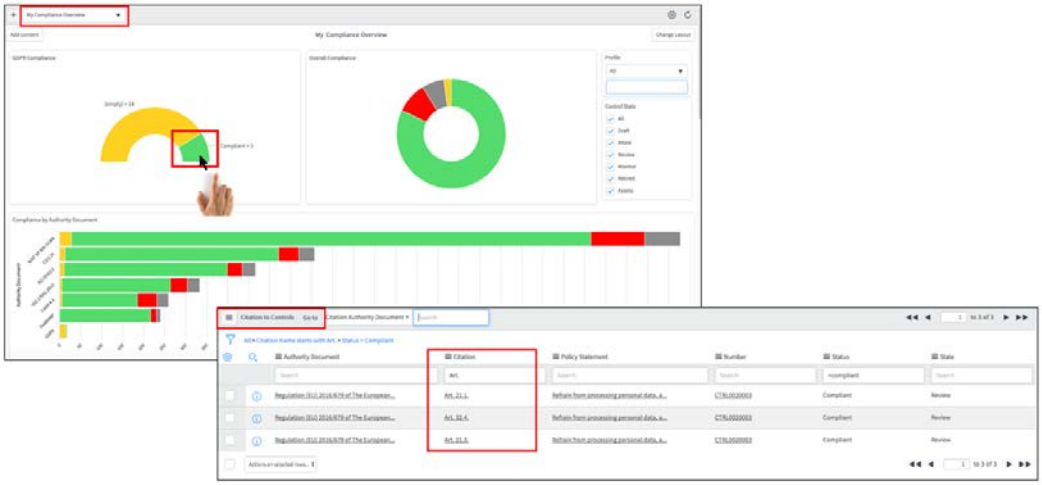


8. Go back to the **Acme Inc. Profile**. Click **Controls**.



9. Depending on your response to that attestation, you see control status as **Compliant** or **Noncompliant.**

10. Return to the Dashboard. (**Compliance Overview**). Refresh your browser.

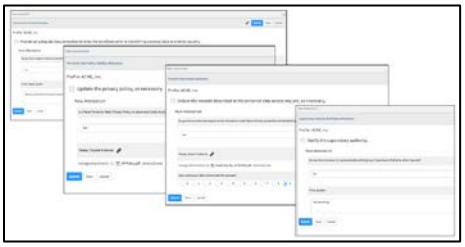


11. See the status of **GDPR Compliance**.

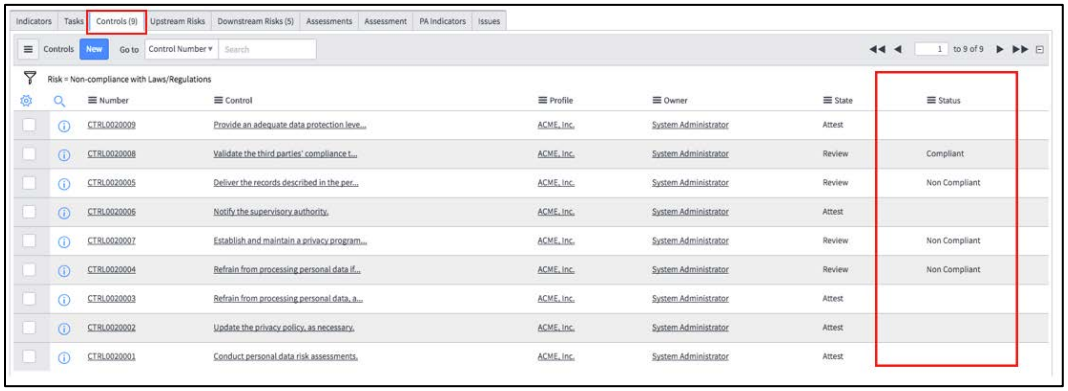
12. Click on the **green part of pie** (or red for non-compliant) of the pie chart in **GDPR Compliance** gauge. There are additional citations related to that particular control in **Compliant/Non-compliant** status.

13. Return to the attestations and take remaining attestations.





14. Check **Controls** status time-to-time and dashboards as in previous steps (next example).



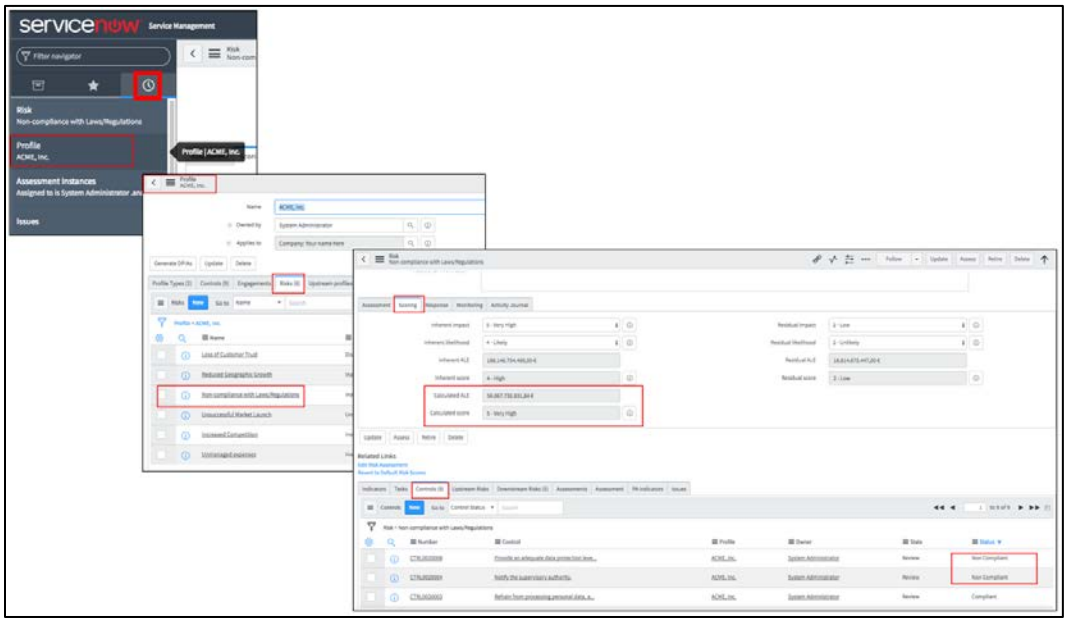
15. Check the **Compliance Overview** Dashboard. Your dashboard might look different than shown below. You may need to refresh your browser window.



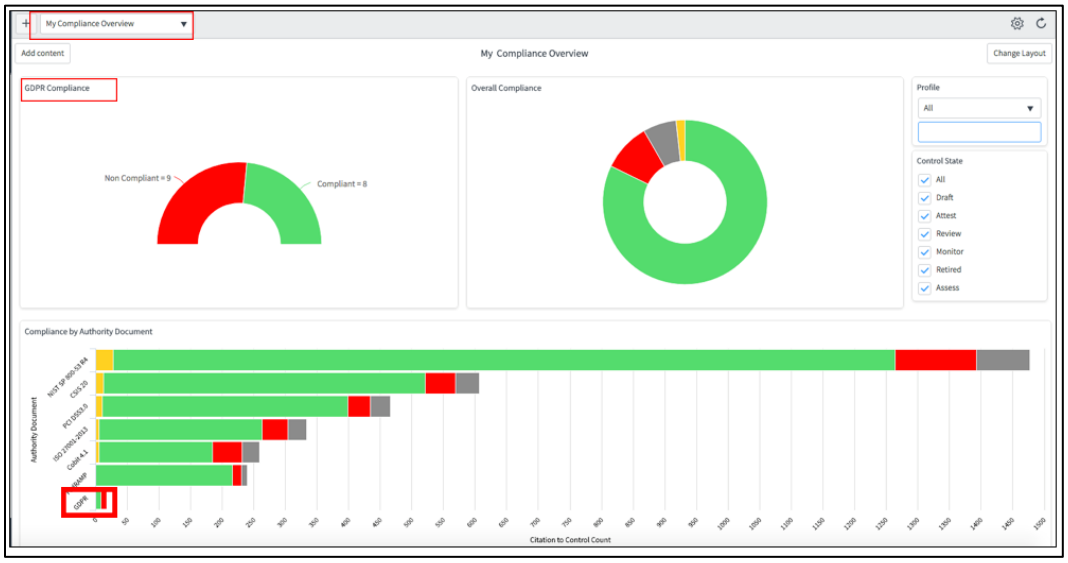
After having 2-3 noncompliant controls, check the risk status as described in following steps:

1. Go to **History** Icon ( ). Select **Profile ACME Inc**.
2. Select **Non-Compliance with Laws/Regulations** risk under the Risk tab in related list.
3. In the **Non-Compliance with Laws/Regulations** Risk window, select **Scoring**.

4. There is a new score for the risk. Because of some noncompliant controls, **Calculated Score** is now higher. You may have a different score than shown below.

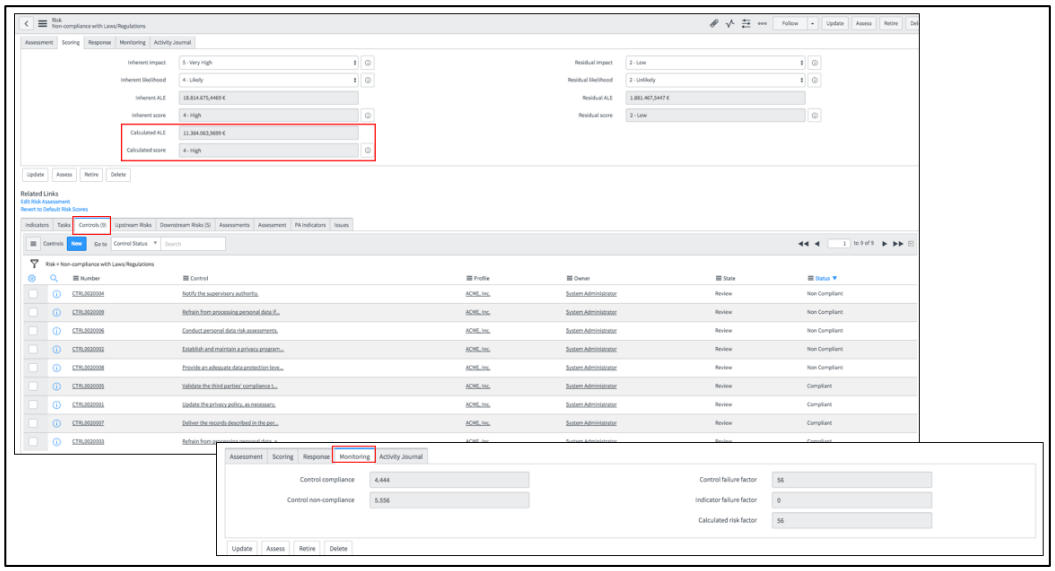


5. After finishing all attestations, go back to the dashboard to see the latest status of **GDPR Compliance**. Your dashboard might be different than shown below.

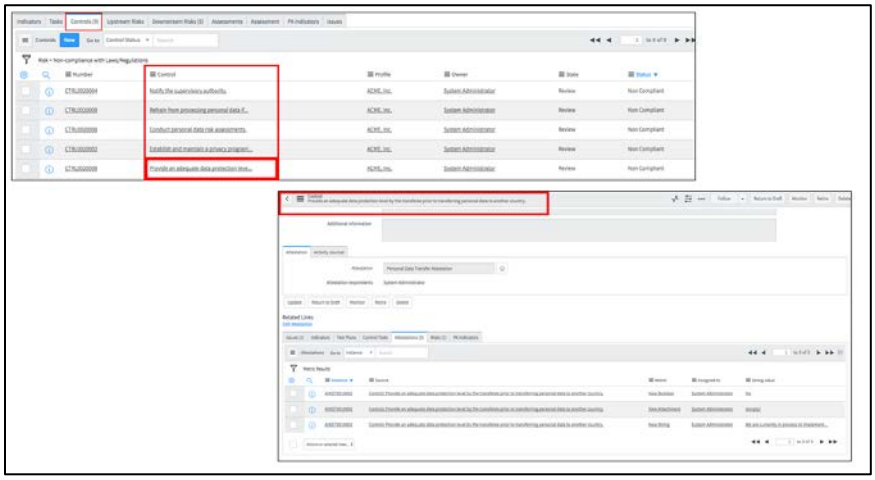


6. Check the final risk **scoring**.

7. Click the **Monitoring** tab to see control compliance metrics.

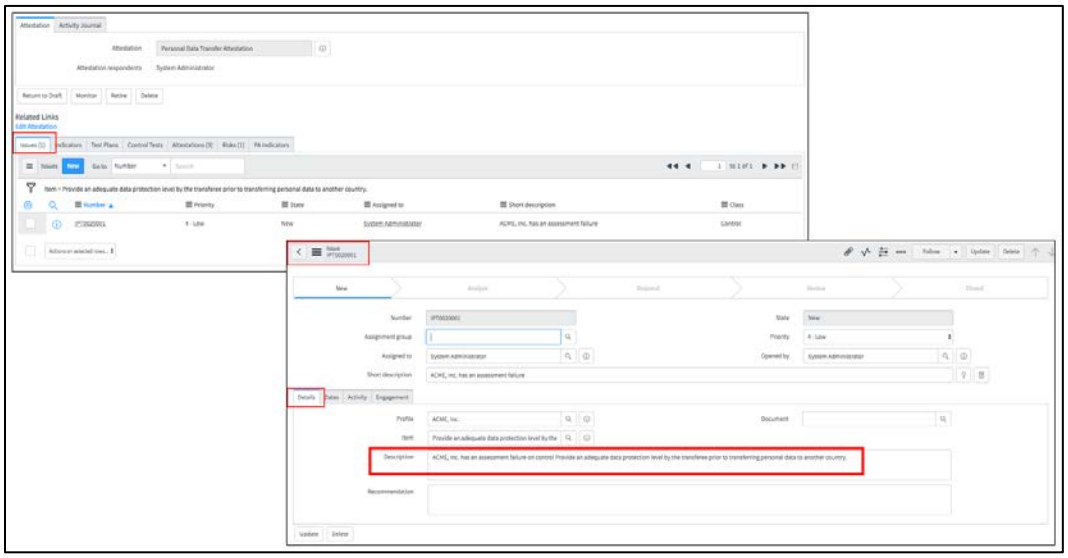


8. Scroll down and go to one of noncompliant control (if you have any) by clicking on the **Controls** tab in related list. Click the **Name** of a noncompliant control.



9. Click the **Issues** tab in the related list. An issue has been automatically generated as result of this noncompliant control. Open the issue record. The record is in **New** state in the Life Cycle (next example).

10. Under Details tab, the reason appears in the **Description** box. Now, an assignee can start working on resolving the issue (not part of this lab).



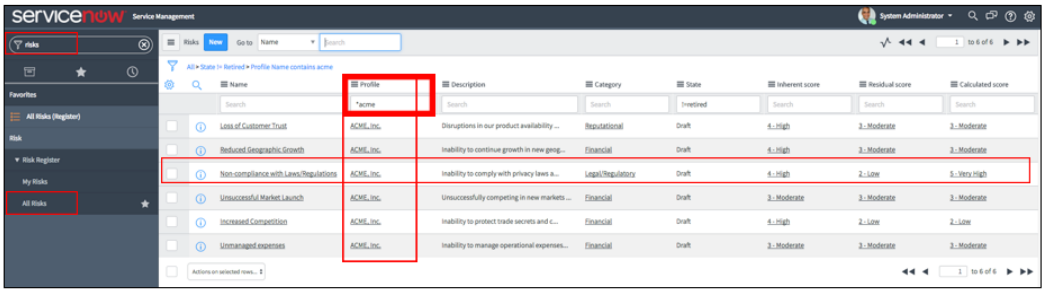
Lab Goal

This lab explains how to create and add new content to the Risk Dashboard to get visibility on high impact risks instantly.

Lab 4
Risk
Dashboard

1. Search for **Risks** in filter navigator.

2. Click **All Risks.** Filter the Risks Records by **Profile: ACME Inc.** as shown below. All the risks related to **ACME Inc**. are listed (not in retired stage). **Non-compliance with Laws/Regulations** is also listed.



3. Make the following changes to see these risks by **Calculated Score** in the Risk Dashboard.

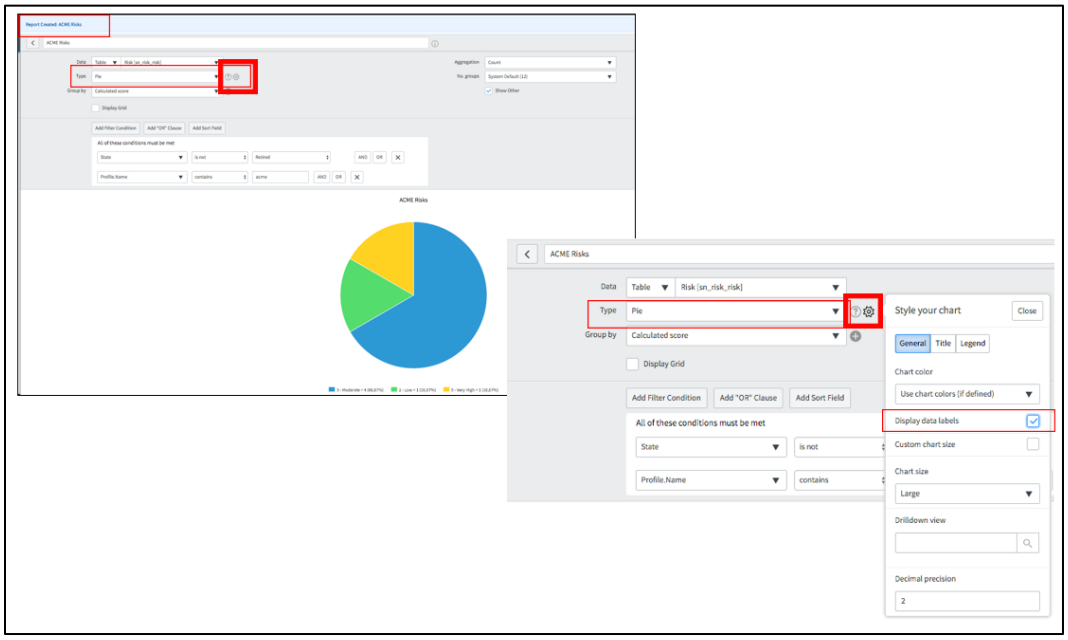


4. Right-click on **Calculated Score** field, then select **Pie Chart.**

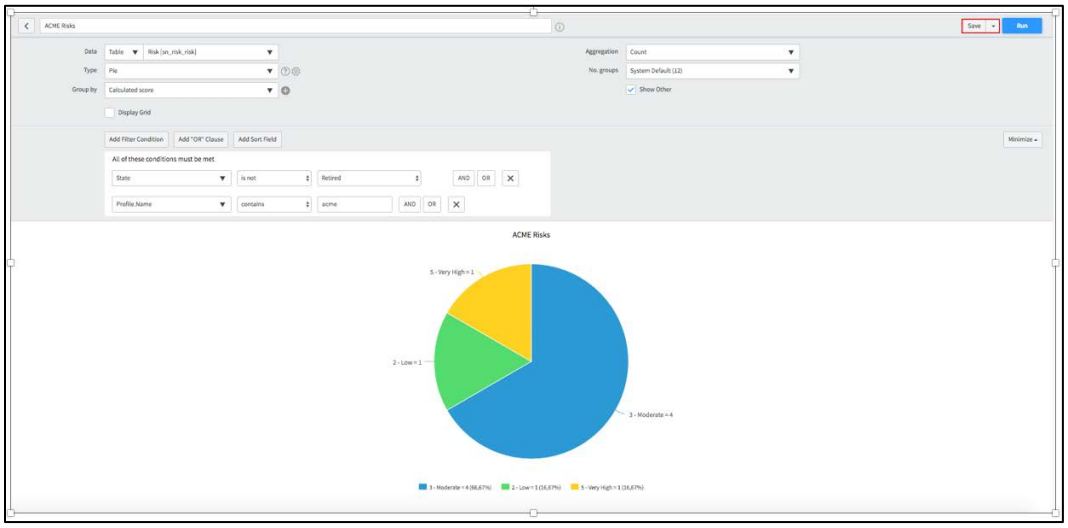


5. A new window opens. Enter the report name in **Report Title** (e.g., **ACME Risks**) field and click **Save**.

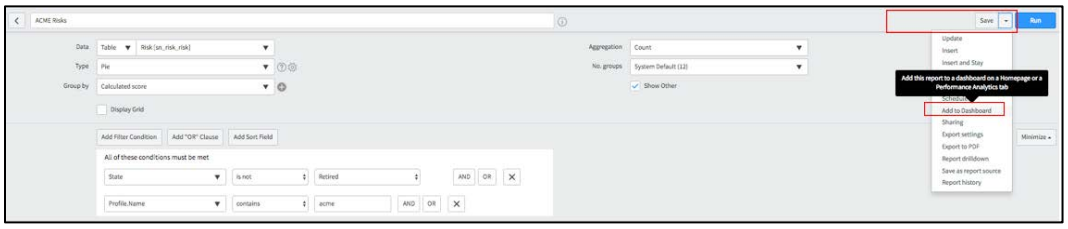
6. Click the **Settings icon** at the end of **Type** field as shown below. Check the box for **Display data labels.** Close window.



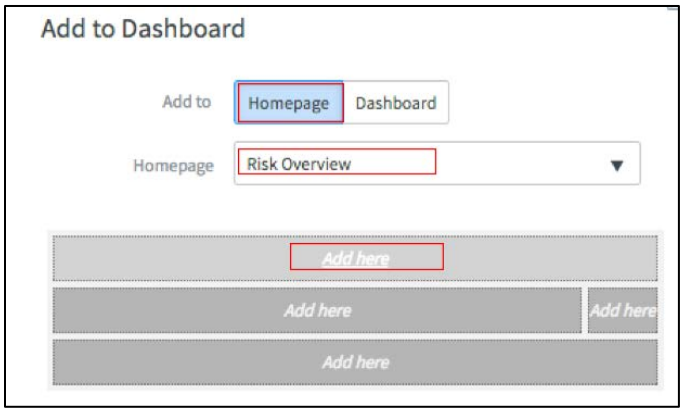
7. Click **Save** at the top right of the report window. See the **ACME Risks** report.



8. Select **Add to Dashboard** from the drop-down list next to **Save** button.



9. Add to the report to your Homepage **(Risk Overview)** as shown below.



10. You are automatically directed to **Risk Overview** homepage.

