

# 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**



This  
Page  
Intentionally  
Left  
Blank

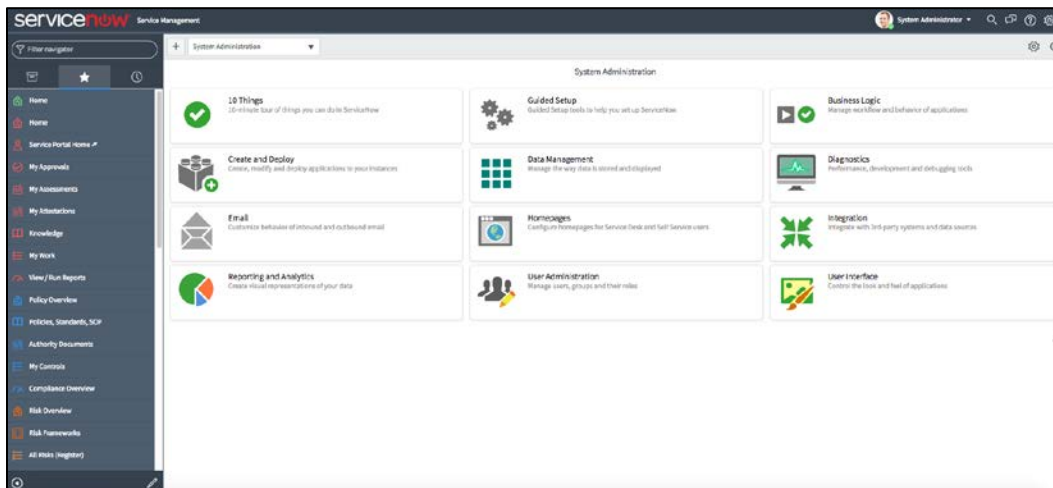
## Lab Goal

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.

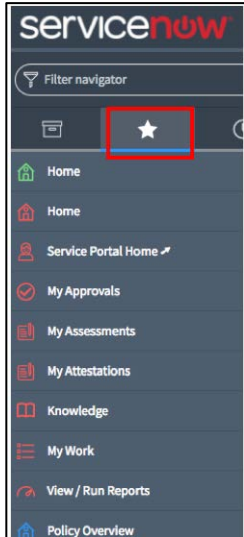
## Lab 1.0 Apps & Dashboard

### Getting Started – Log on to Your Training Instance

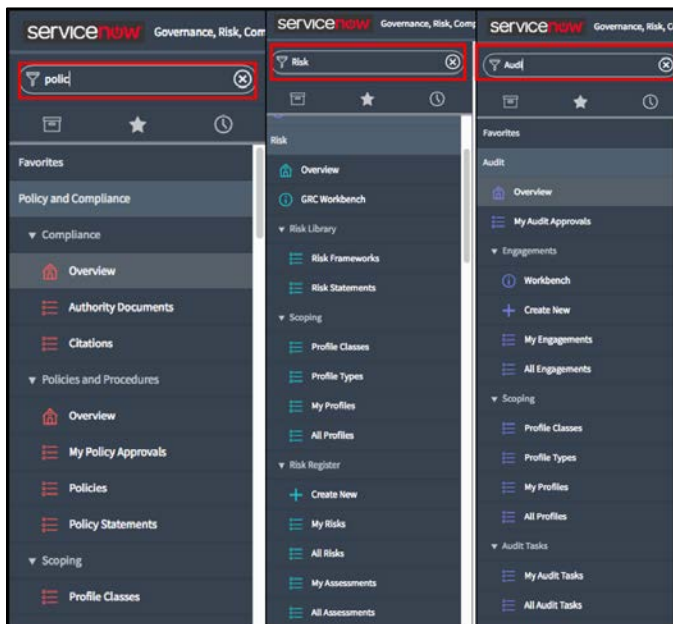
1. Navigate to the unique instance URL provided to you.
2. Log on with the provided credentials.
3. See your homepage.



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

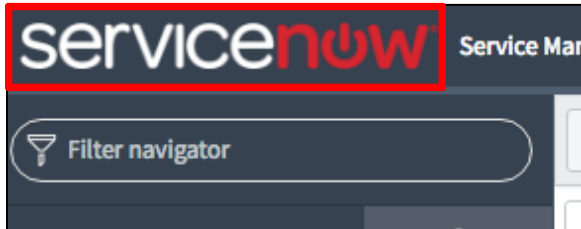


- Discover GRC applications and its modules by typing first few letters of **Policy & Compliance**; **Risk Management & Audit Management**.

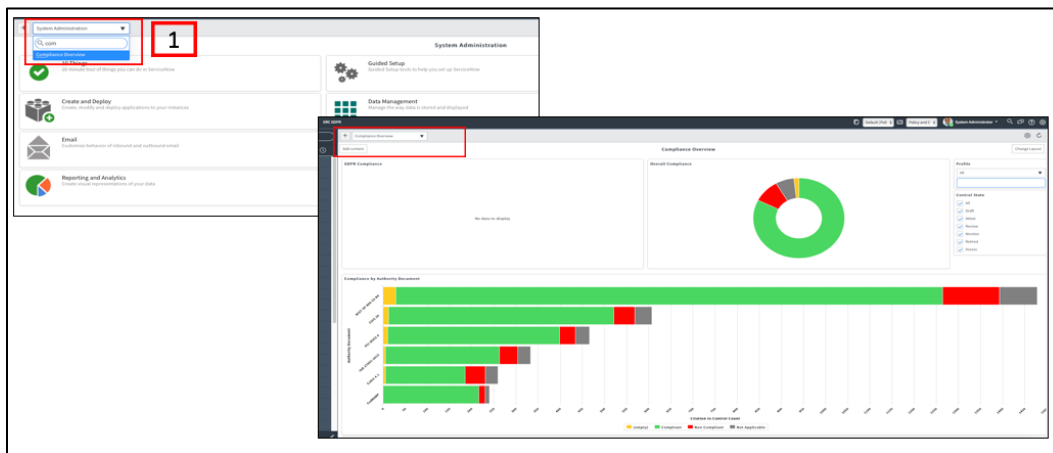


## Check Your Homepage

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.

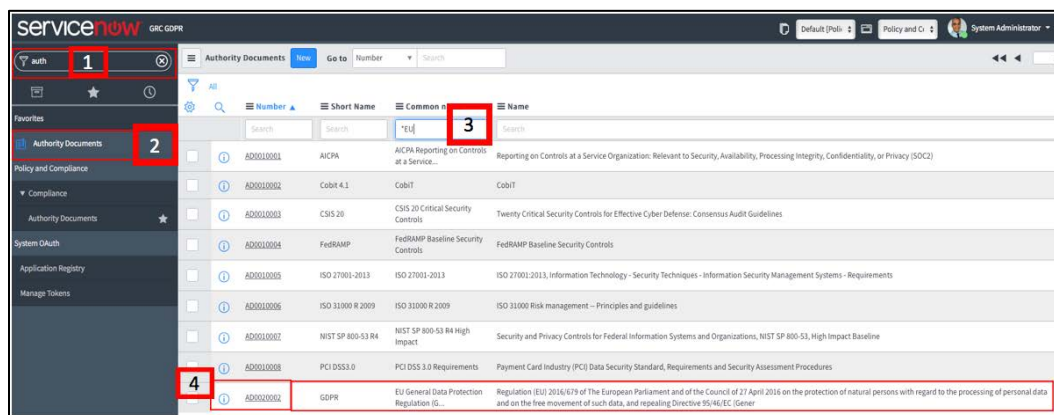
## Lab Goal

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

### 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.

## Lab 1.1 Authority Document GDPR



**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.

AD0000006	ISO 31000 R 2009	ISO 31000 Risk management - Principles and guidelines	International or National Standard
AD0000007	NIST SP 800-53 R4 High Impact	Security and Privacy Controls for Federal Information Systems and Organizations, NIST SP 800-53, High Impact Baseline	International or National Standard
AD0000008	PCI DSS 3.0 Requirements	Payment Card Industry (PCI) Data Security Standard, Requirements and Security Assessment Procedures	Self-Regulatory Body Requirement
AD0000009	EU General Data Protection Regulation (G...)	Regulation (EU) 2016/679 of The European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)	Regulation or Statute

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.

**Authority Document**

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data, and repealing Directive 95/46/EC (General Data Protection Regulation)

Update ↑ ↓

Name	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC		
Number	AD000003	Source ID	D003802
Location	LCF	Version	
Common name	EU General Data Protection Regulation	Valid from	
Category	Europe	Valid to	
Type	Regulations		
URL	<a href="http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=urisrv:eu_l_2016_119_01_01_EN&amp;doc=CGLI%2016_119_TOC">http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=urisrv:eu_l_2016_119_01_01_EN&amp;doc=CGLI%2016_119_TOC</a>		
Description	European Union. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), issued by EUR-Lex.		
	This document has a type of "Regulation" and is assigned as LCF AD 0000002 as a part of the Europe category. This document's availability is "Free". It was originally found online at <a href="http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=urisrv:eu_l_2016_119_01_01_EN&amp;doc=CGLI%2016_119_TOC">http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=urisrv:eu_l_2016_119_01_01_EN&amp;doc=CGLI%2016_119_TOC</a> .		
	This Authority Document has 1221 citations mapped to EEF LCF Common Contexts. The document as a whole was last reviewed and released on 2023-03-17.		

Update Delete

Citations (1,021) Views

Citations [04] [Views]

Buttons: Citation Reference Annotate

Authority Document - Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (name = Reference = Annotate)

Search Reference Annotate Description

Search

- [Annotate] [04,35] Data protection impact assessment
- [Reference] [04,35,1] Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall prior to the processing... of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address all similar processing operations that present similar high risks.
- [Annotate] [04,35,10] When processing pursuant to point (c) or (e) of Article 6(1) has a legal basis in Union law or in the law of the Member State(s) in which the controller is subject, that law requires the specific processing operation or set of operations in question, and a data protection impact assessment has already been carried out as part of a general impact assessment in the context of the adoption of that legal basis, paragraph 1 is to apply not unless Member States deem it to be necessary to carry out such an assessment prior to processing activities.
- [Annotate] [04,35,11] Where necessary, the controller shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least where there is a change of the risk represented by processing operations.
- [Annotate] [04,35,2] The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment.
- [Annotate] [04,35,3] A data protection impact assessment referred to in paragraph 1 shall be performed by the case officer.
- [Annotate] [04,35,3(a)] a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect his or her situation;
- [Annotate] [04,35,3(b)] processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10, or
- [Annotate] [04,35,3(c)] a systematic monitoring of a publicly accessible area on a large scale.
- [Annotate] [04,35,4] The supervisory authority shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1. The supervisory authority shall

## 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

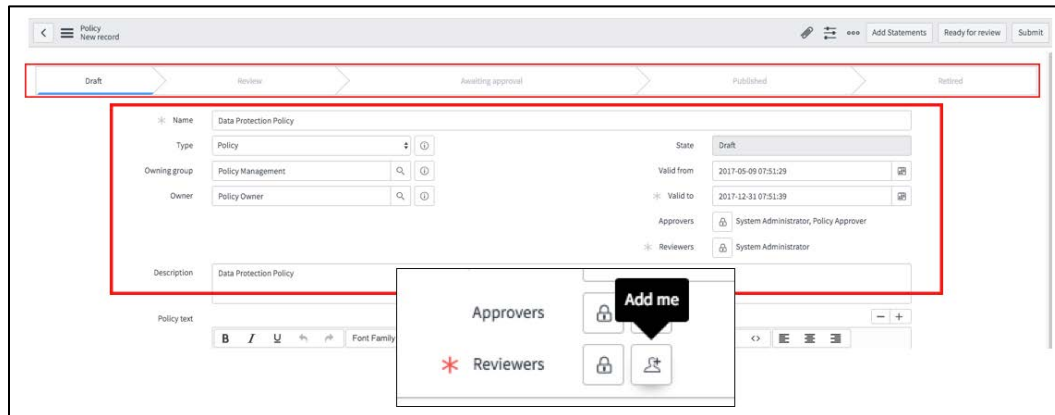
1. Go to **Policy & Management** application.
2. Look for **Policies**. Click **Policies** to list them.
3. Click **New** at the top of the policies page.

Number	Name	Type	State	KB article
POL0010000	Environmental Control Management policy	Policy	Published	X80010004
POL0010010	Business Records and Media Management	Policy	Published	X80090008
POL0010013	Remote Access Control policy	Policy	Published	X80010006
POL0010045	Intrusion and Incident Response Standard Operating Procedure	Plan	Awaiting approval	
POL0010047	Facility Management policy	Policy	Published	X80010005
POL0010091	Operating System Access Management policy	Policy	Review	X80010007
POL0010021	Change Management	Standard	Published	X80090032
POL0020001	Organizational Segregation of Duties	Standard	Published	X80090006
POL0020005	Business Protection Policy	Standard	Published	X80090015
POL0020007	Risk Management Policy	Policy	Published	X80090033
POL0020008	Security Response Plan	Standard	Published	X80090012
POL0020009	Acceptable Use Policy	Standard	Published	X80090014
POL0020013	Disaster Recovery Policy (BCDR)	Policy	Published	X80090021

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



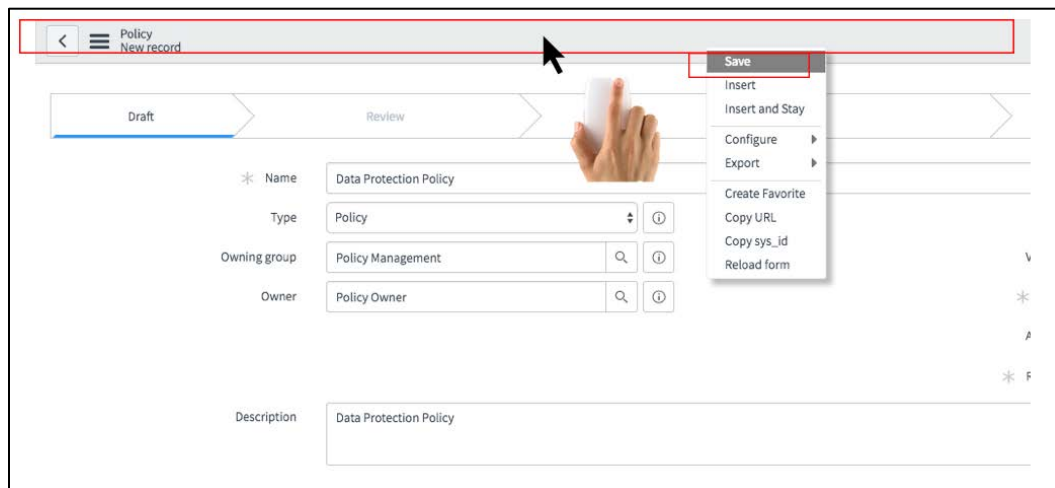
5. Fill out **New Policy Record** as shown. You can click on  icon to add yourself (**System Administrator**) or click on the lock icon to add **Policy Approver**.



The screenshot shows the 'New Policy Record' form in ServiceNow. The form is in the 'Draft' state. A red box highlights the main form fields. A modal window is open over the 'Reviewers' section, showing an 'Add me' button and a lock icon.

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

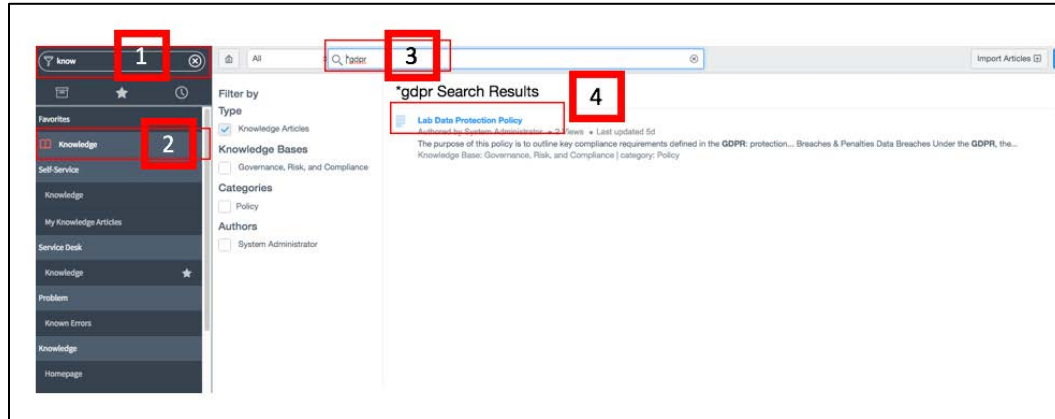
6. To save the record, right-click on the **Policy Record bar**, open the drop-down menu, and click **Save**.



The screenshot shows the 'New Policy Record' form in ServiceNow. A red box highlights the top bar. A hand is shown right-clicking on the bar, and a context menu is open with the 'Save' option highlighted.

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

## 8. Click **Knowledge** application.

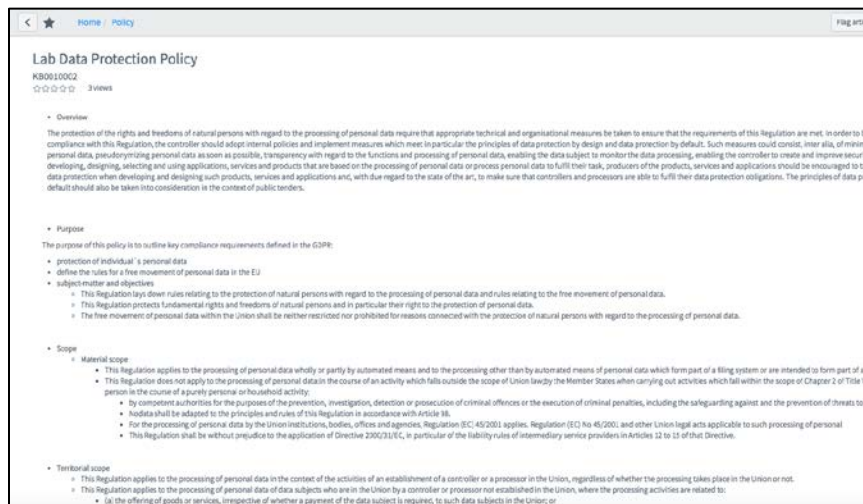


## 9. Search for **\*gdpr** in the search bar.

## 10. You see a Lab Data Protection Policy.

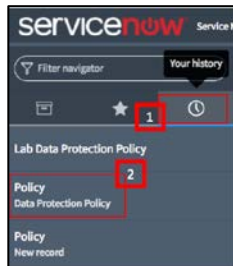
## 11. Open the **Policy**.

## 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).

**Overview**

The protection of the rights and freedoms of natural persons with regard to the processing of personal data require that appropriate technical and organizational measures be taken to ensure that the requirements of this Regulation are met. In order to be able to demonstrate compliance with this Regulation, the controller should adopt internal policies and measures which relate to particular the protection of data protection by design and data protection by default. Such measures could consist, inter alia, of minimizing the processing of personal data, pseudonymizing personal data as soon as possible, minimizing the retention of personal data, ensuring the data subject's right to access the data processing, ensuring the controller to enable and improve security measures, when developing, designing, testing and using, adopting, services and products that are based on the processing of personal data or provide personal data to third parties, evaluation of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations. The principle of data protection by design and by default should also be taken into consideration in the context of public bodies.

**Purpose**

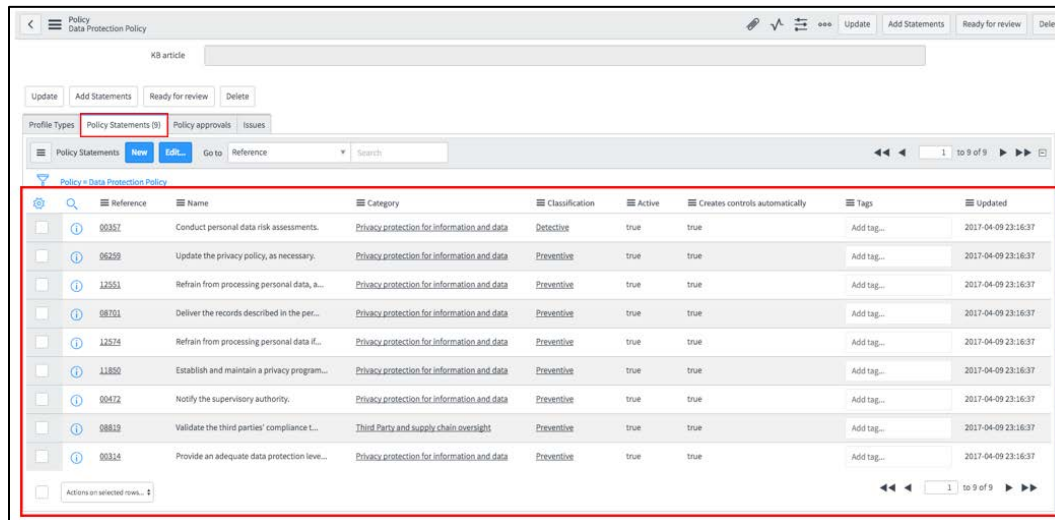
The purpose of this policy is to outline key compliance requirements defined in the GDPR:

- protection of individual's personal data
- define the rules for a free movement of personal data in the EU
- establish member and employees
- This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.
- This Regulation protects fundamental rights and freedoms of natural persons and, in particular, their right to the protection of personal data.
- This Regulation also establishes the responsibilities of controllers and processors of personal data in relation to such protection.

Now assign relevant Policy Statements to the Policy.

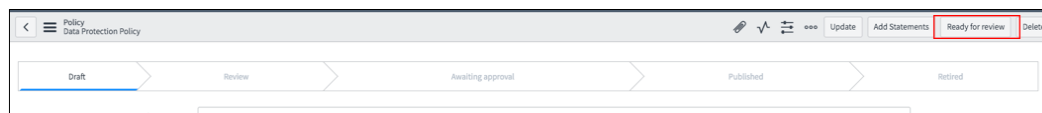
1. Generate Policy Statements that are defined for the policy by clicking **Add Statements**.

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



	Reference	Name	Category	Classification	Active	Creates controls automatically	Tags	Updated
<input type="checkbox"/>	00357	Conduct personal data risk assessments.	Privacy protection for information and data	Detective	true	true	Add tag...	2017-04-09 23:16:37
<input type="checkbox"/>	06259	Update the privacy policy, as necessary.	Privacy protection for information and data	Preventive	true	true	Add tag...	2017-04-09 23:16:37
<input type="checkbox"/>	12551	Refrain from processing personal data, a...	Privacy protection for information and data	Preventive	true	true	Add tag...	2017-04-09 23:16:37
<input type="checkbox"/>	08701	Deliver the records described in the per...	Privacy protection for information and data	Preventive	true	true	Add tag...	2017-04-09 23:16:37
<input type="checkbox"/>	12578	Refrain from processing personal data if...	Privacy protection for information and data	Preventive	true	true	Add tag...	2017-04-09 23:16:37
<input type="checkbox"/>	11850	Establish and maintain a privacy program...	Privacy protection for information and data	Preventive	true	true	Add tag...	2017-04-09 23:16:37
<input type="checkbox"/>	00472	Notify the supervisory authority.	Privacy protection for information and data	Preventive	true	true	Add tag...	2017-04-09 23:16:37
<input type="checkbox"/>	08819	Validate the third parties' compliance t...	Third Party and supply chain oversight	Preventive	true	true	Add tag...	2017-04-09 23:16:37
<input type="checkbox"/>	00314	Provide an adequate data protection leve...	Privacy protection for information and data	Preventive	true	true	Add tag...	2017-04-09 23:16:37

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 2<sup>nd</sup> example.

This screenshot shows the 'Data Protection Policy' form in the 'Review' state. The 'Request Approval' button is highlighted with a red box in the top right corner. The form fields are as follows:

Field	Value
Name	Data Protection Policy
Type	Policy
Owning group	Policy Management
Owner	Policy Owner
State	Review
Valid from	2017-04-09 23:05:38
Valid to	2017-04-30 23:05:41
Approvers	System Administrator, Policy Approver
Reviewers	System Administrator

This screenshot shows the 'Data Protection Policy' form in the 'Review' state, where all fields are read-only. The form fields are as follows:

Field	Value
Name	Data Protection Policy
Type	Policy
Owning group	Policy Management
Owner	Policy Owner
State	Review
Valid from	2017-04-13 01:32:09
Valid to	2017-12-31 01:32:19
Approvers	Policy Approver, Nitin Rudrawar
Reviewers	Nitin Rudrawar
Description	Data Protection Policy
Policy text	<ul style="list-style-type: none"> <li>Overview                     <p>The protection of the rights and freedoms of natural persons with regard to the processing of personal data require that appropriate technical and organisational measures be taken to ensure that the requirements of this Regulation are met. In order to be able to demonstrate compliance with this Regulation, the controller should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default. Such measures could consist, inter alia, of minimising the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features. When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations. The principles of data protection by design and by default should also be taken into consideration in the context of public tenders.</p> </li> <li>Purpose                     <p>The purpose of this policy is to outline key compliance requirements defined in the GDPR:</p> <ul style="list-style-type: none"> <li>protection of individual's personal data</li> <li>define the rules for a free movement of personal data in the EU</li> <li>subject matter and objectives                             <ul style="list-style-type: none"> <li>This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.</li> <li>This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.</li> </ul> </li> </ul> </li> </ul>

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

The screenshot shows the 'Policy Data Protection Policy' form. At the top, a progress bar indicates the current state is 'Awaiting approval', with previous states 'Draft' and 'Review' marked as complete. The form fields include:

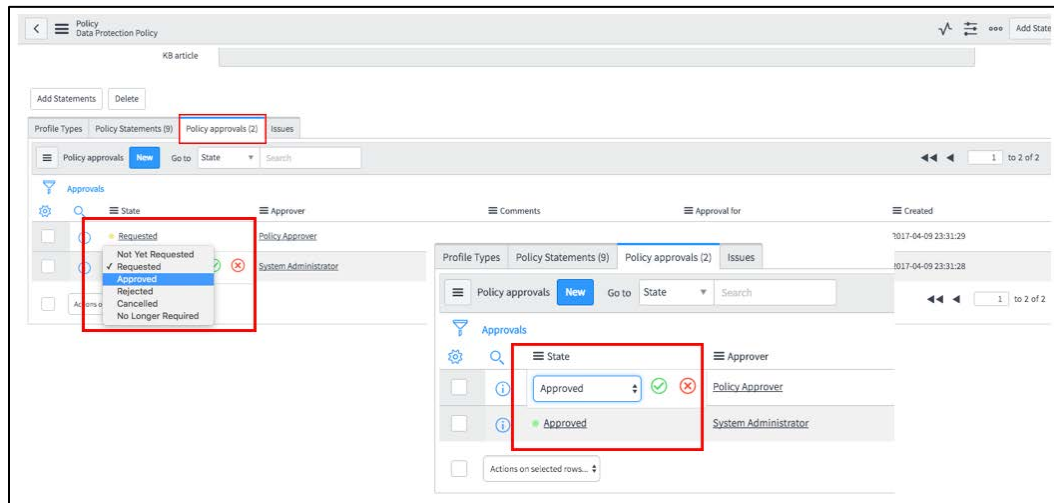
- Name:** Data Protection Policy
- Type:** Policy
- Owning group:** Policy Management
- Owner:** Policy Owner
- State:** Awaiting approval
- Valid from:** 2017-04-09 23:05:38
- Valid to:** 2017-04-30 23:05:41
- Approvers:** System Administrator, Policy Approver
- Reviewers:** System Administrator
- Description:** Data Protection Policy
- Policy text:** Overview
  - The protection of the rights and freedoms of natural persons with regard to the processing of personal data require that appropriate technical and organisational measures be taken to ensure that the requirements of this Regulation are met. In order to be able to demonstrate compliance with this Regulation, the controller should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default. Such measures could consist, inter alia, of minimizing the processing of personal data, pseudonymizing personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features. When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations. The principles of data protection by design and by default should also be taken into consideration in the context of public tenders.

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

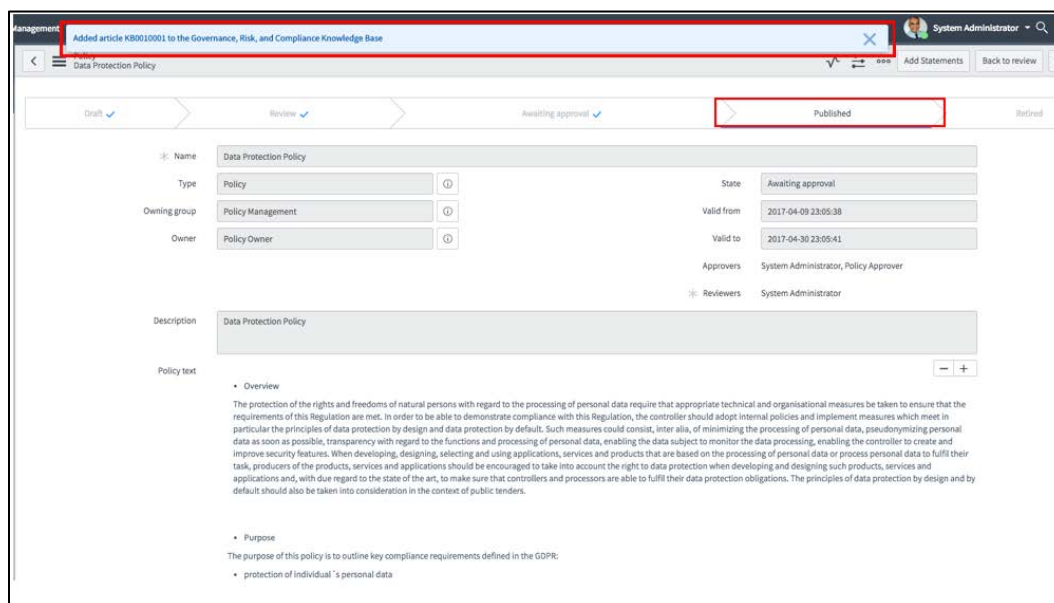
The screenshot shows the 'Policy Approvals' list. The 'Policy approvals (2)' tab is selected. The list has columns for State, Approver, Comments, Approval for, and Created. A dropdown menu is open for the first row, showing options: Requested, Not Yet Requested, Requested, Approved, Rejected, Cancelled, and No Longer Required. The second row is highlighted.

State	Approver	Comments	Approval for	Created
Requested	Policy Approver			2017-04-09 23:31:29
Requested	System Administrator			2017-04-09 23:31:28


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

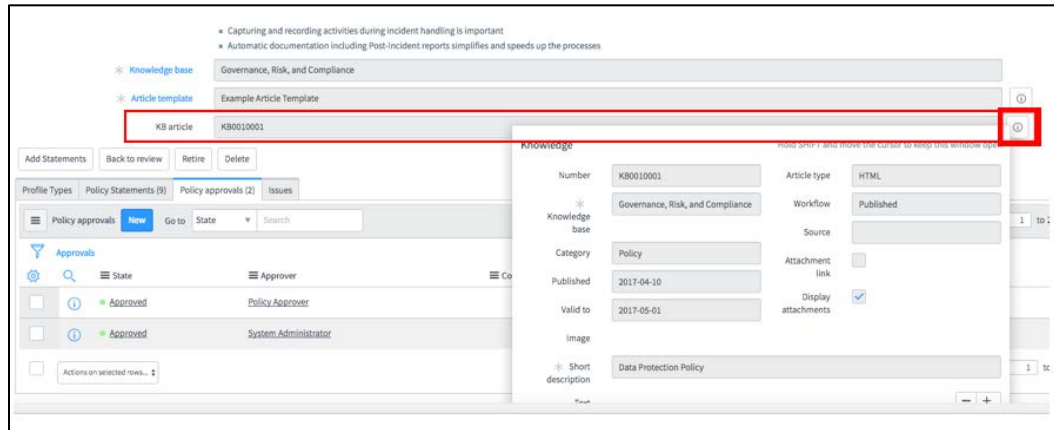


- Reload form. The Policy Record has moved to state **Published**. Also, a Knowledge Article has been published.

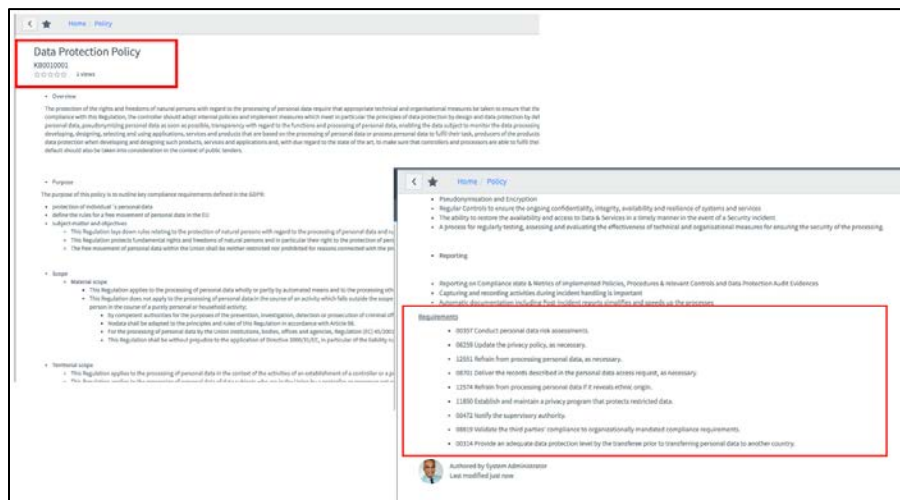




6. Scroll to **KB Article** and click the information  icon at the end of the line.



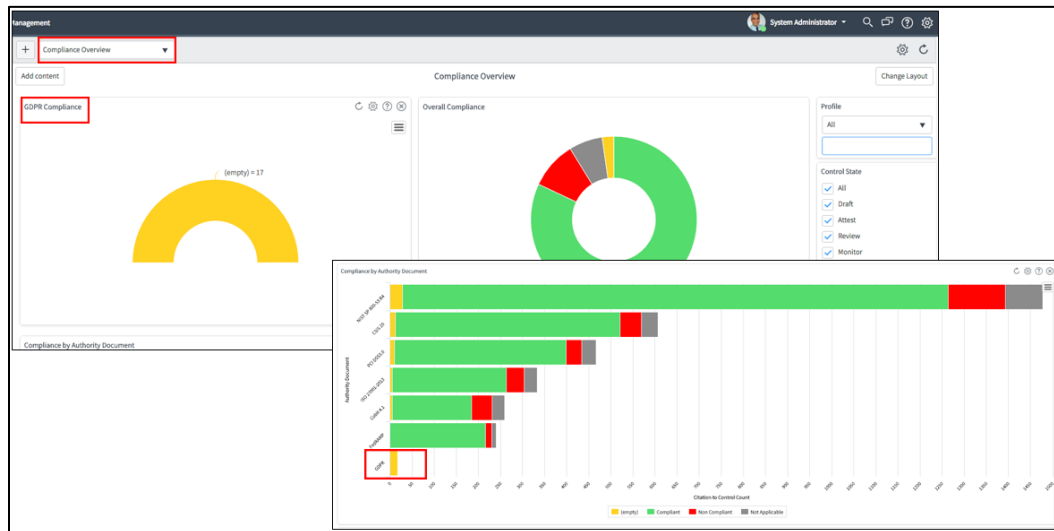
7. A Knowledge record window opens. Scroll to **View Article** under **Related links** in this record.
8. Click **View Article**.
9. See the KB-Article that has been created automatically with related requirements listed at the bottom of the article.



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.



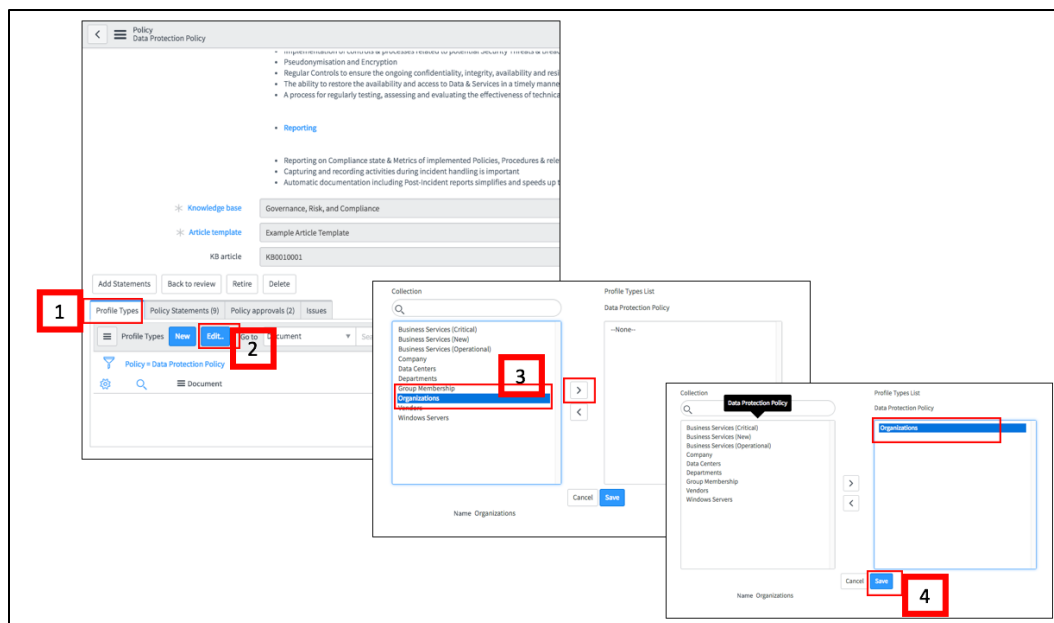
## Lab Goal

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

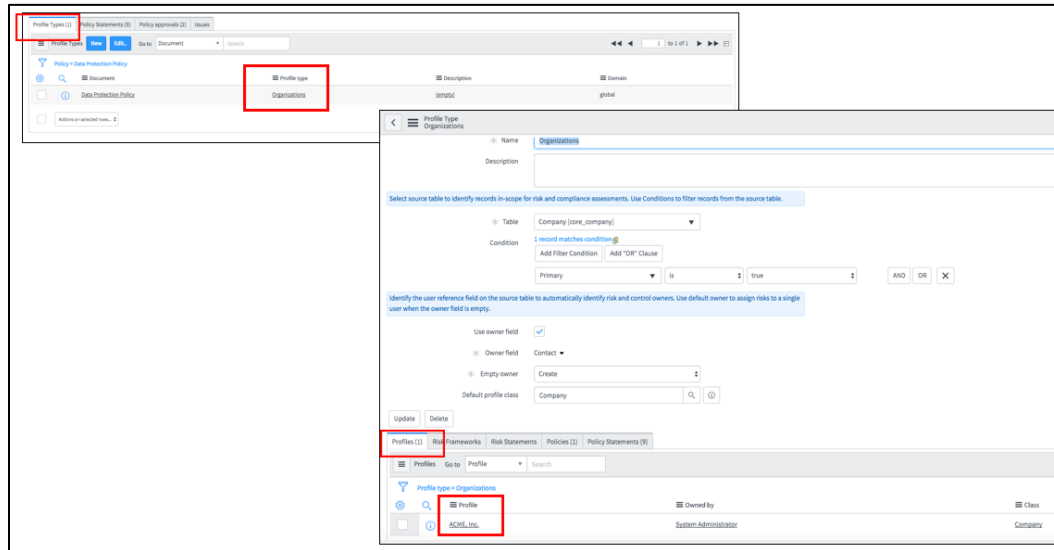
### Profile Type, Profile & Risk Framework

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**.

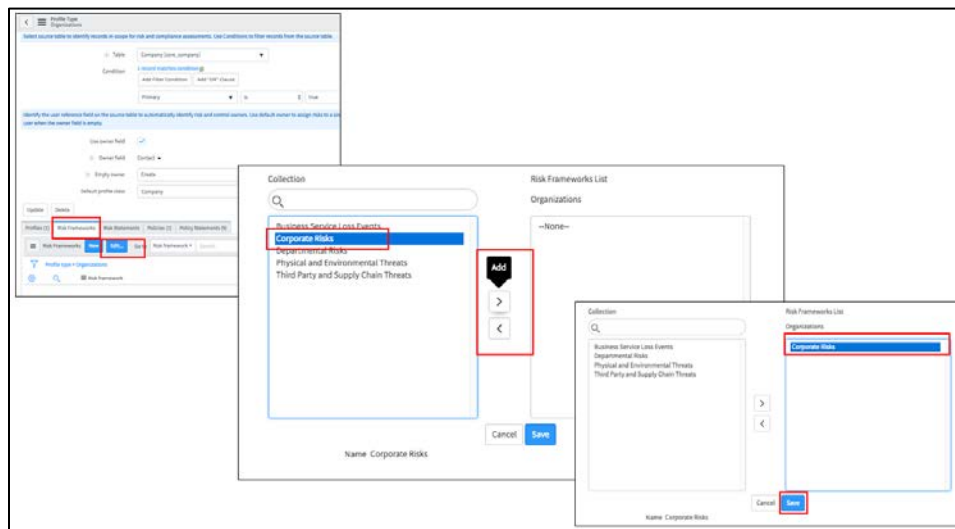


4. Click **Organizations**, move it into right window, and click **Save**.
5. You return to the Policy record. Scroll down and click on **Organizations** under **Profile Type** related list.

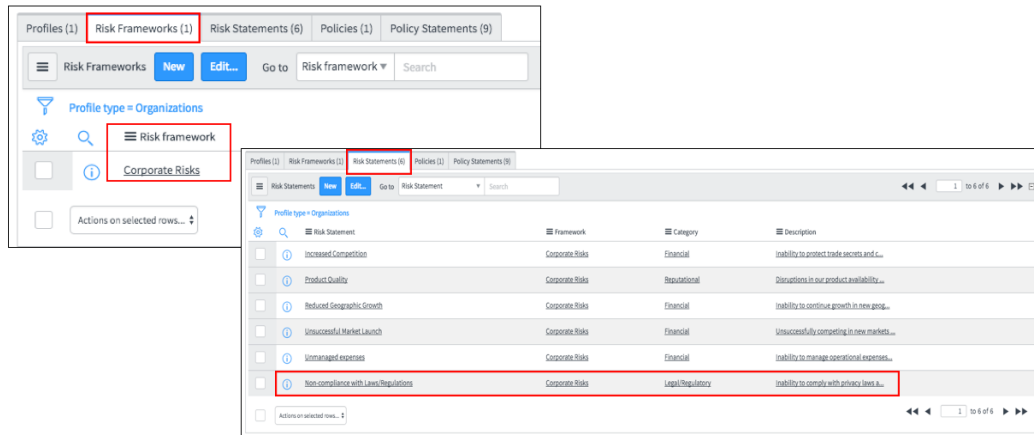
6. **Profile Type** record opens in a new window. A **Profile, ACME Inc.**, is assigned to this Profile Type.



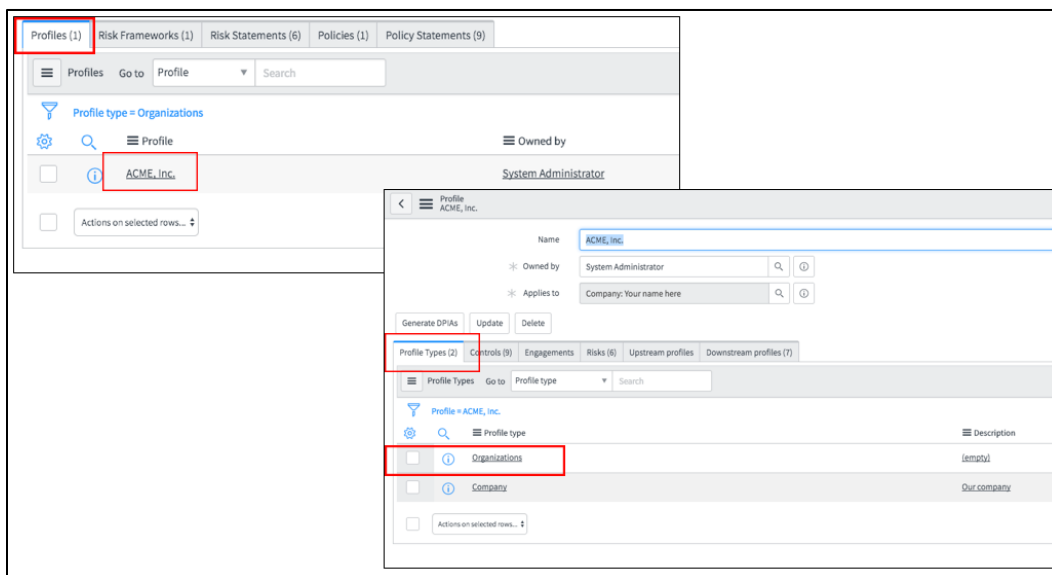
7. **Policies & Policy Statements** appear in the related list, created in earlier steps.
8. Now, add **Risk Framework** to the **Profile Type** as shown below. Add **Corporate Risks** to Profile type and click **Save**.



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

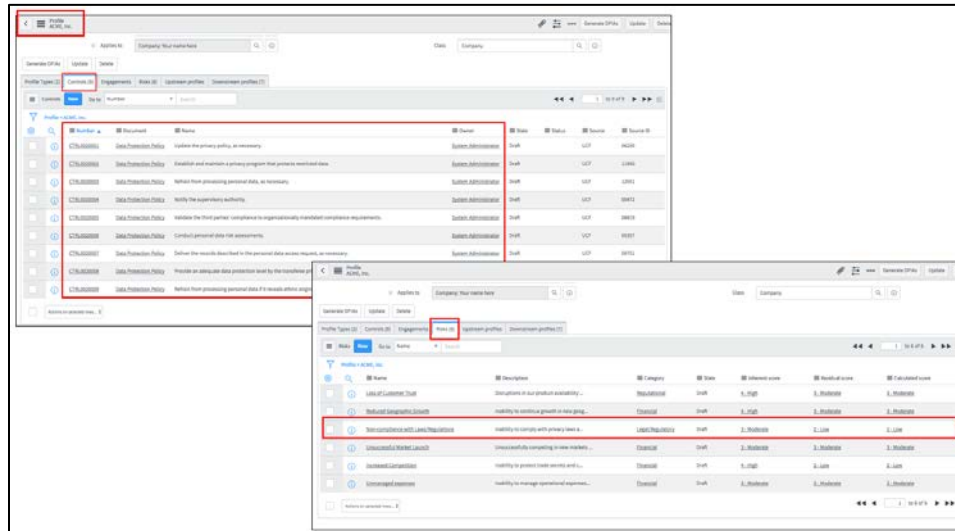


10. Click on **Risk Statements** to see assigned **Risk Statements**.
11. You should have some **Risk Statements**, including **Non-compliance with Law/ Regulations**. You revisit this **Risk Statement** later.
12. Return to **Profile** under Related lists. Click on Profile **ACME Inc.**



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

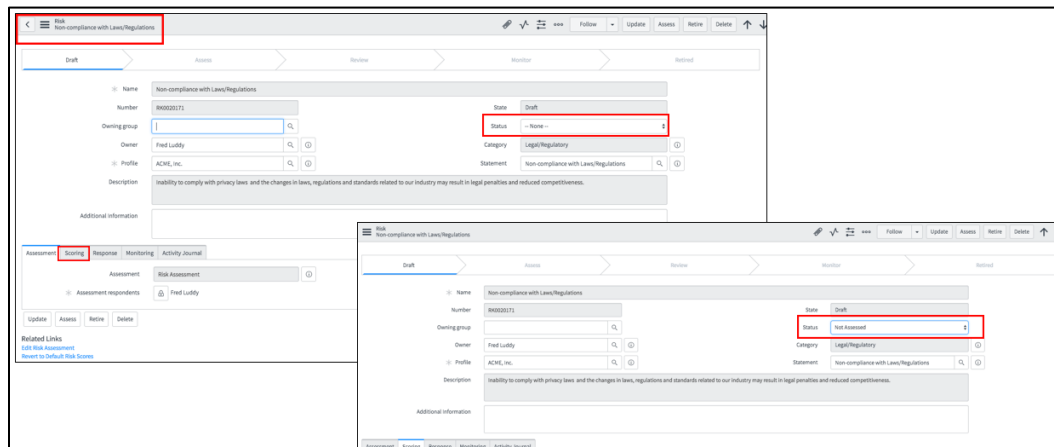
14. Click the **Controls** tab, next to **Profile Type**. There are 9 controls allocated to this **Profile** as requirements described in the Policy.



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.

**Risk: Non-compliance with Laws/Regulations**

Draft | Assess | Review | Monitor | Retire

Name: Non-compliance with Laws/Regulations  
 Number: R00202171  
 State: Draft  
 Status: Not Assessed  
 Owner: Fred Luby  
 Category: Legal/Regulatory  
 Profile: ACME, Inc.  
 Statement: Non-compliance with Laws/Regulations  
 Description: Inability to comply with privacy laws and the changes in laws, regulations and standards related to our industry may result in legal penalties and reduced competitiveness.

**Assessment** | Scoring | Response | Monitoring | Activity Journal

Inherent impact: 3 - Moderate  
 Inherent likelihood: 3 - Neutral  
 Inherent ALE: 0.00 \$  
 Inherent score: 3 - Moderate  
 Calculated ALE: 0.00 \$  
 Calculated score: 2 - Low

Residual impact: 3 - Moderate  
 Residual likelihood: 2 - Unlikely  
 Residual ALE: 0.00 \$  
 Residual score: 2 - Low

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

**Assessment** | Scoring | Response | Monitoring | Activity Journal

Inherent impact: 5 - Very High  
 Inherent likelihood: 4 - Likely  
 Inherent ALE: 18,814,675,446 \$  
 Inherent score: 4 - High  
 Calculated ALE: 1,881,467,544 \$  
 Calculated score: 2 - Low

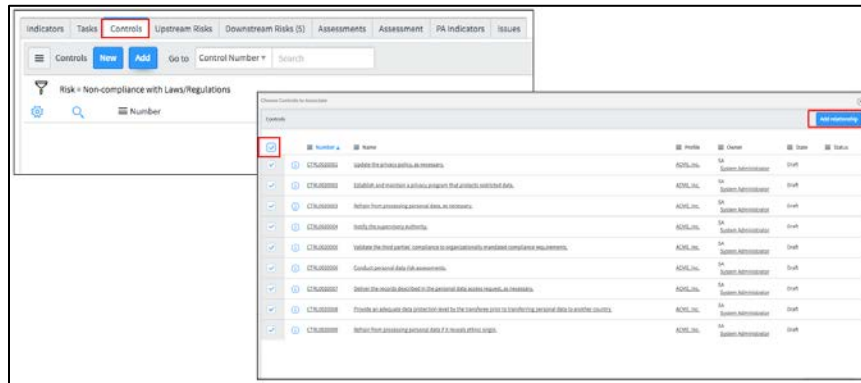
Residual impact: 2 - Low  
 Residual likelihood: 2 - Unlikely  
 Residual ALE: 1,881,467,544 \$  
 Residual score: 2 - Low

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

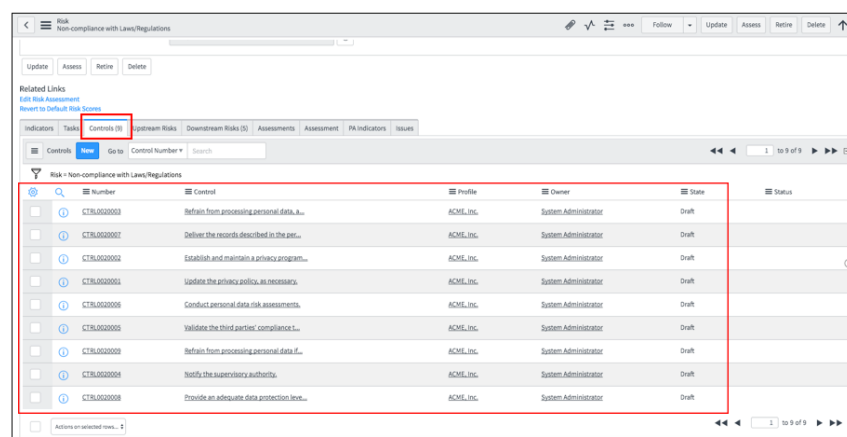
Add controls to associate GDPR requirements to the risk.

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.

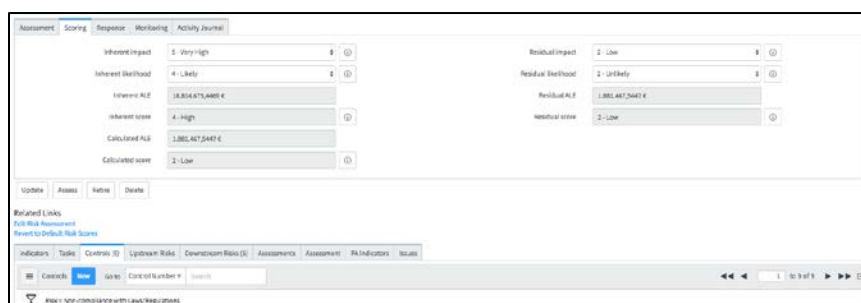
### 3. Select All controls and click **Add Relationship**.



### 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.

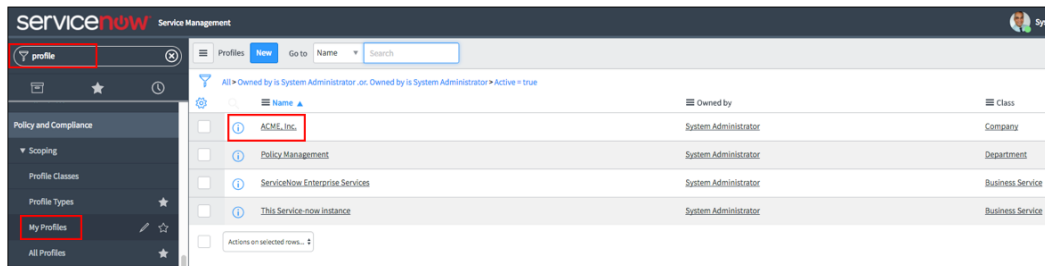


## Lab Goal

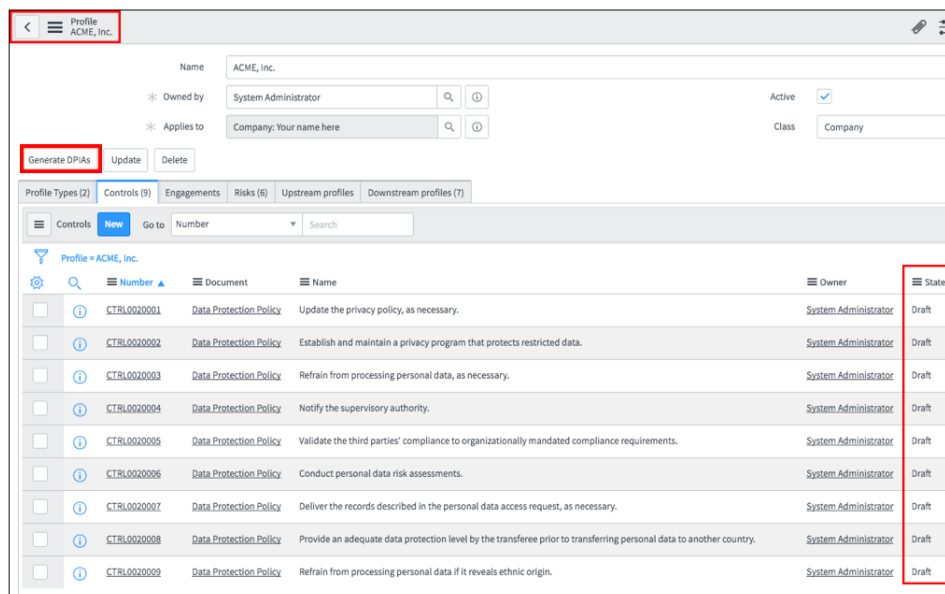
This lab explains how to generate attestations for Data Protection requirements described in the Policy for the ACME Inc. Depending on attestations responses, controls status changes from draft to compliant or noncompliant and has an effect on risk scoring.

## Lab 3.0 Attestations

1. Return to your **Profile**.

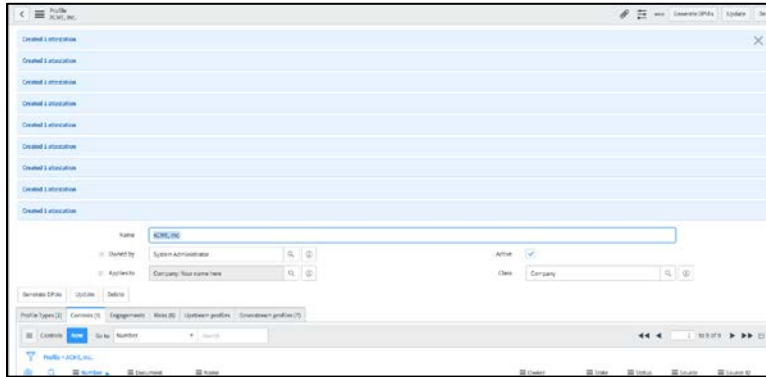


2. Click **ACME Inc.**
3. Click **Generate DPIAs** (Data Protection Impact Assessments).

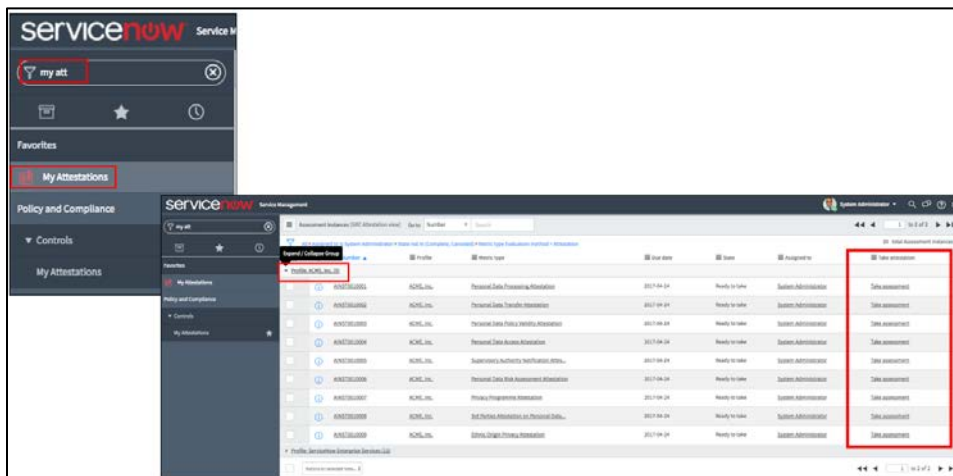




- There are 9 created **attestations**.



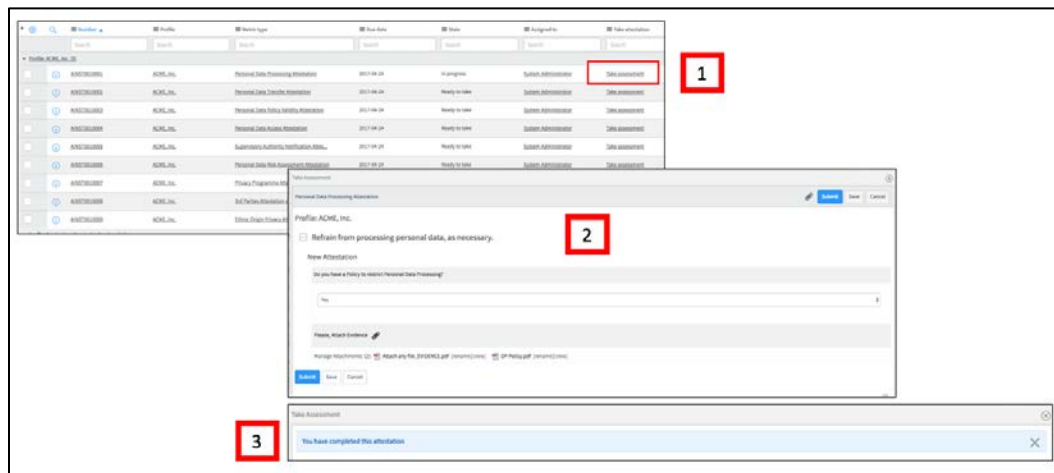
- Search in filter navigator for **My Attestations** and click it.



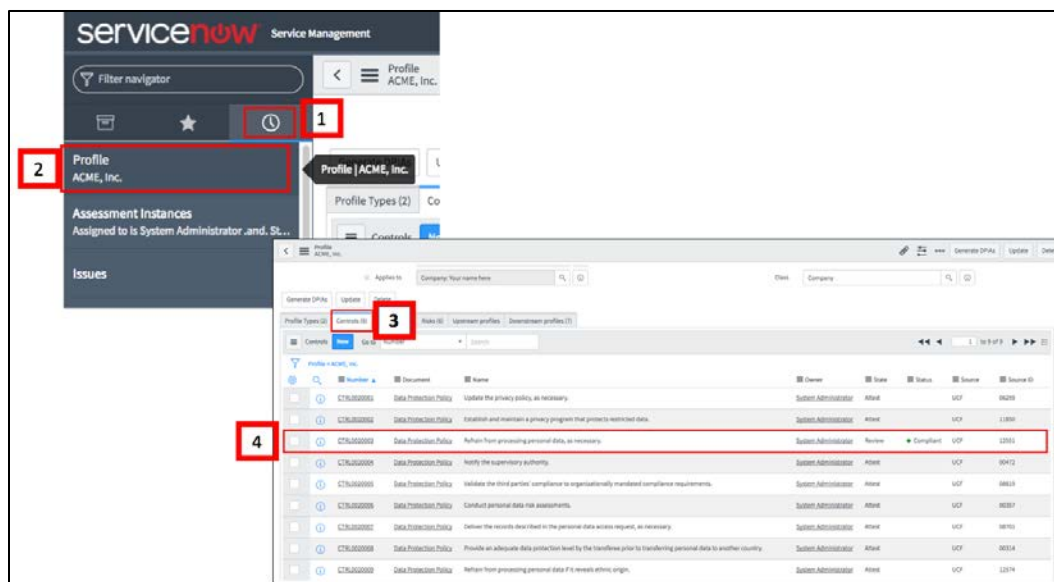
- Expand the **Profile ACME Inc.** to see full record. You should have now 9 attestations in **Ready to Take** state.

Go to Dashboard. It should be yellow.

- 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.

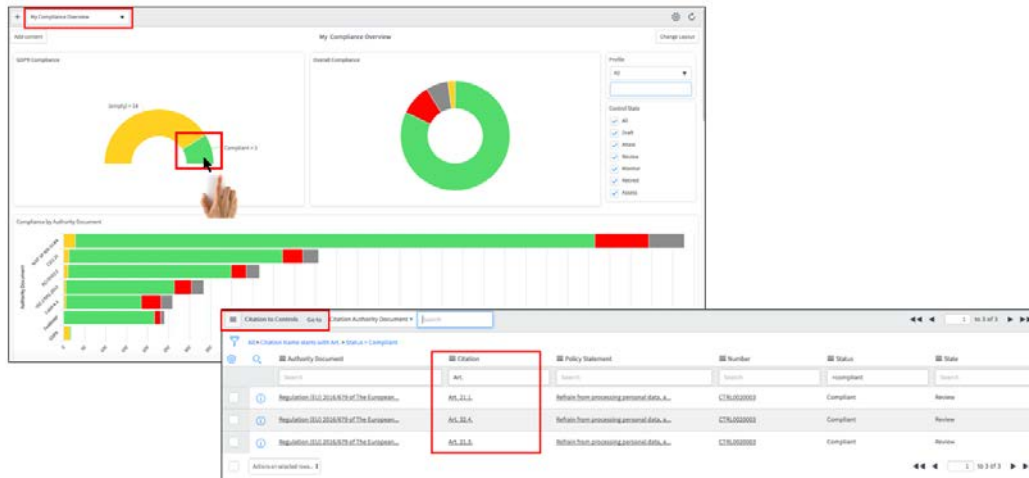


- Go back to the **Acme Inc. Profile**. Click **Controls**.



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

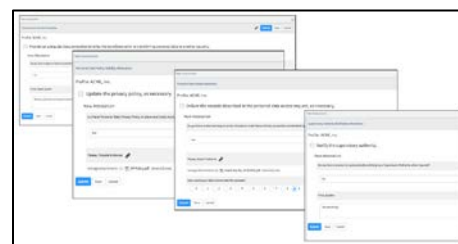
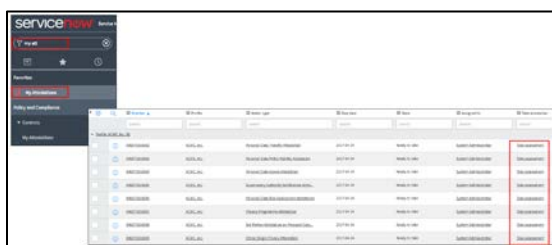
10. Return to the Dashboard. (**Compliance Overview**). Refresh your browser.



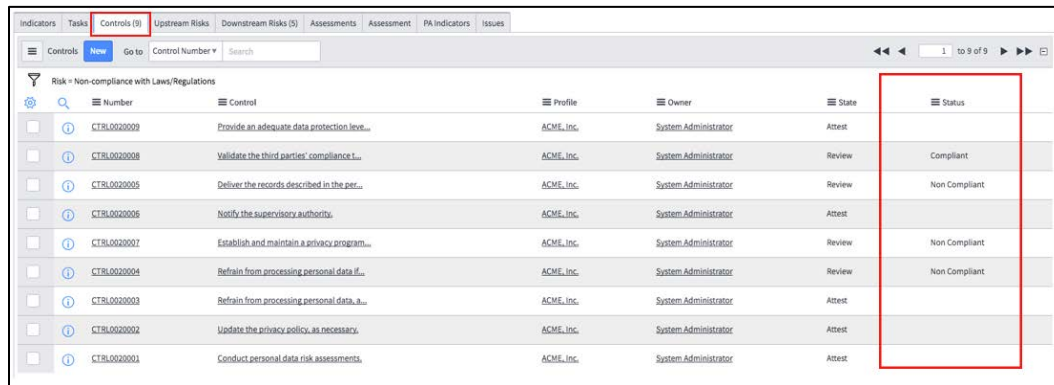
11. See the status of **GDPR Compliance**.

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).



Number	Control	Profile	Owner	State	Status
CTBL002009	Provide an adequate data protection level...	ACME, Inc.	System Administrator	Attest	Non Compliant
CTBL002008	Validate the third parties' compliance...	ACME, Inc.	System Administrator	Review	Compliant
CTBL002005	Deliver the records described in the per...	ACME, Inc.	System Administrator	Review	Non Compliant
CTBL002006	Notify the supervisory authority.	ACME, Inc.	System Administrator	Attest	Non Compliant
CTBL002007	Establish and maintain a privacy program...	ACME, Inc.	System Administrator	Review	Non Compliant
CTBL002004	Refrain from processing personal data if...	ACME, Inc.	System Administrator	Review	Non Compliant
CTBL002003	Refrain from processing personal data, a...	ACME, Inc.	System Administrator	Attest	Non Compliant
CTBL002002	Update the privacy policy, as necessary,	ACME, Inc.	System Administrator	Attest	Non Compliant
CTBL002001	Conduct personal data risk assessments,	ACME, Inc.	System Administrator	Attest	Non Compliant

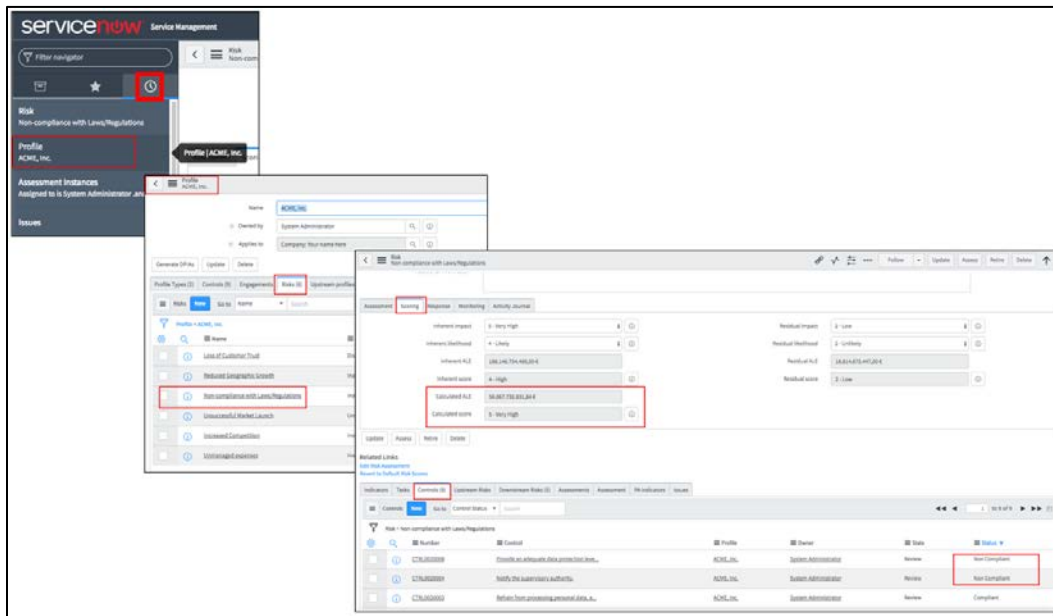
15. Check the **Compliance Overview** Dashboard. Your dashboard might look different than shown below. You may need to refresh your browser window.



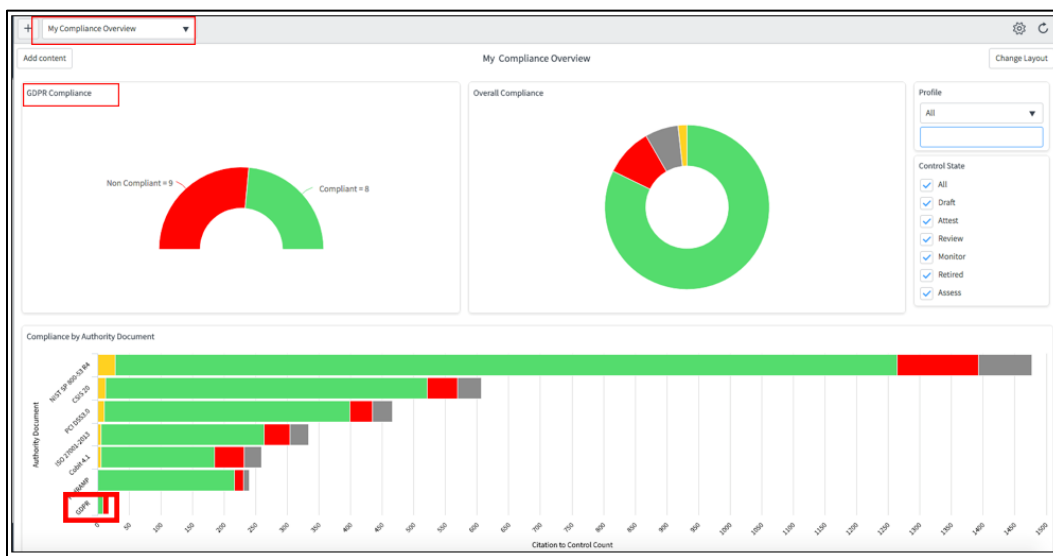
After having 2-3 noncompliant controls, check the risk status as described in following steps:

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**.

- 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.



- 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.



- Check the final risk **scoring**.

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

The screenshot displays the Risk Management System (RMS) interface, specifically the 'Risk Assessment' tab. The interface is divided into several sections:

- Top Navigation Bar:** Includes tabs for 'Assessment', 'Scoring', 'Response', 'Monitoring', and 'Activity Journal'. The 'Monitoring' tab is currently selected and highlighted in red.
- Assessment Form:** Located at the top, it contains fields for 'Inherent impact', 'Inherent likelihood', 'Inherent ALE', 'Residual impact', 'Residual likelihood', 'Residual ALE', and 'Residual score'. The 'Inherent ALE' and 'Residual score' fields are highlighted with red boxes.
- Related Links:** A section below the assessment form containing links like 'Risk Assessment' and 'Default Risk Score'.
- Indicators Section:** A table listing various indicators with columns for 'Number', 'Description', 'Profile', 'Owner', 'Status', and 'Review'. The 'Monitoring' tab is highlighted in the bottom navigation bar.
- Bottom Navigation Bar:** Includes tabs for 'Assessment', 'Scoring', 'Response', 'Monitoring', and 'Activity Journal'. The 'Monitoring' tab is currently selected and highlighted in red.

The 'Monitoring' tab is highlighted in the top navigation bar, and the 'Monitoring' tab is also highlighted in the bottom navigation bar.

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.

[illegible]

- 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).

- 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).

The screenshot displays the ServiceNow interface for a new incident. The 'Details' tab is active, and the 'Description' field is highlighted with a red box. The field contains the text: 'ACME, Inc. has an assessment failure on control. Provide an adequate data protection level by the transform prior to transferring personal data to another country.'

Other visible fields include:

- Number:** IT0000001
- Assignment group:** System Administrator
- Assigned to:** System Administrator
- Short description:** ACME, Inc. has an assessment failure
- State:** New
- Priority:** 4 - Low
- Opened by:** System Administrator
- Profile:** ACME, Inc.
- Open:** Provide an adequate data protection level by the
- Recommendation:** (Empty field)

## 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.

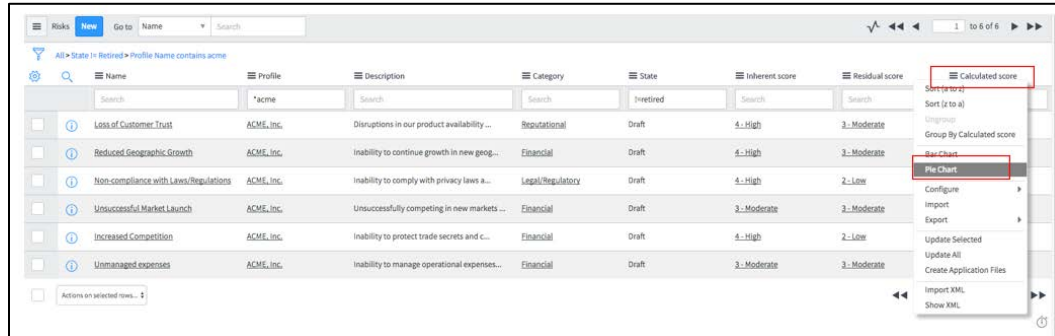
Name	Profile	Description	Category	State	Inherent score	Residual score	Calculated score
Loss of Customer Trust	ACME, Inc.	Disruptions in our product availability...	Reputational	Draft	4..High	3..Moderate	3..Moderate
Reduced Geographic Growth	ACME, Inc.	Inability to continue growth in new geog...	Financial	Draft	6..High	3..Moderate	3..Moderate
Non-compliance with Laws/Regulations	ACME, Inc.	Inability to comply with privacy laws a...	Legal/Regulatory	Draft	4..High	2..Low	5..Very high
Unsuccessful Market Launch	ACME, Inc.	Unsuccessfully competing in new markets ...	Financial	Draft	3..Moderate	3..Moderate	3..Moderate
Increased Competition	ACME, Inc.	Inability to protect trade secrets and c...	Financial	Draft	4..High	2..Low	2..Low
Unmanaged expenses	ACME, Inc.	Inability to manage operational expenses...	Financial	Draft	3..Moderate	3..Moderate	3..Moderate

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

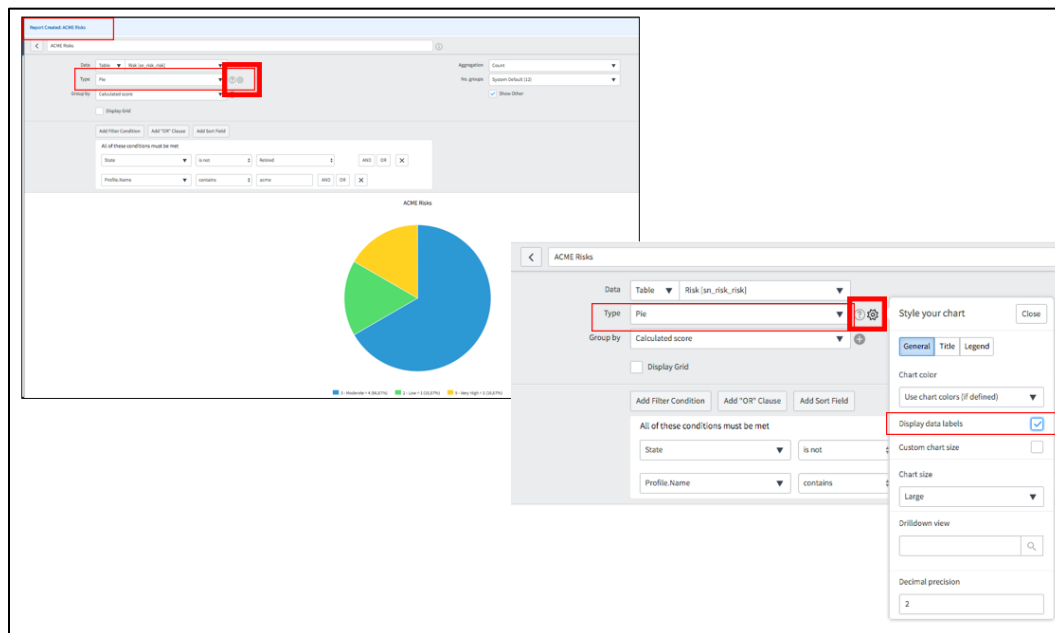
Name	Profile	Description	Category	State	Inherent score	Residual score	Calculated score
Loss of Customer Trust	ACME, Inc.	Disruptions in our product availability...	Reputational	Draft	4..High	3..Moderate	3..Moderate
Reduced Geographic Growth	ACME, Inc.	Inability to continue growth in new geog...	Financial	Draft	6..High	3..Moderate	3..Moderate
Non-compliance with Laws/Regulations	ACME, Inc.	Inability to comply with privacy laws a...	Legal/Regulatory	Draft	4..High	2..Low	5..Very high
Unsuccessful Market Launch	ACME, Inc.	Unsuccessfully competing in new markets ...	Financial	Draft	3..Moderate	3..Moderate	3..Moderate
Increased Competition	ACME, Inc.	Inability to protect trade secrets and c...	Financial	Draft	4..High	2..Low	2..Low
Unmanaged expenses	ACME, Inc.	Inability to manage operational expenses...	Financial	Draft	3..Moderate	3..Moderate	3..Moderate



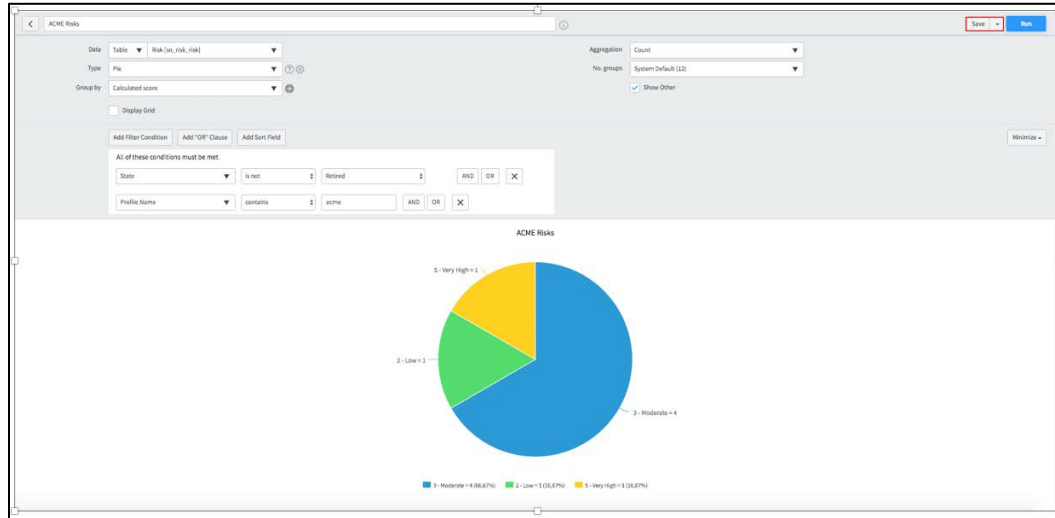
- Right-click on **Calculated Score** field, then select **Pie Chart**.



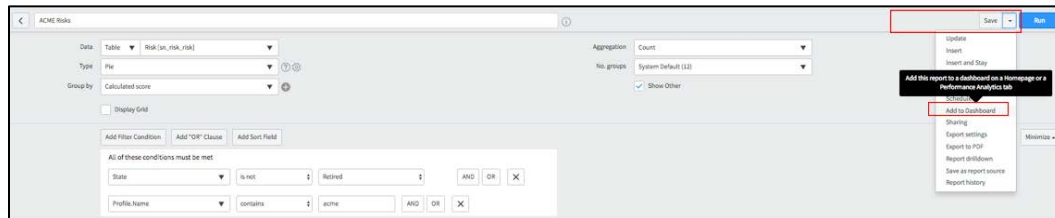
- A new window opens. Enter the report name in **Report Title** (e.g., **ACME Risks**) field and click **Save**.
- Click the **Settings** icon at the end of **Type** field as shown below. Check the box for **Display data labels**. Close window.



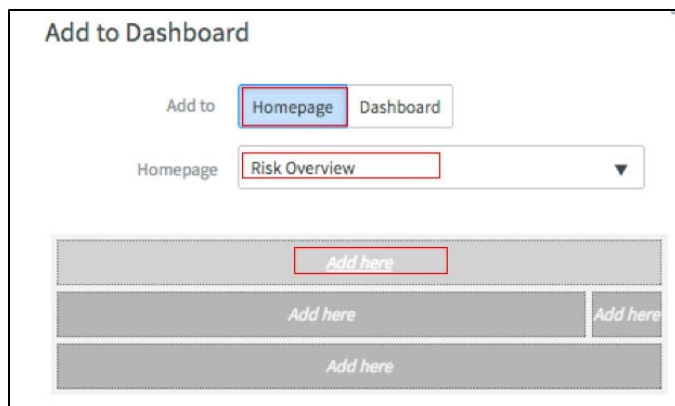
- Click **Save** at the top right of the report window. See the **ACME Risks** report.



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



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



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

