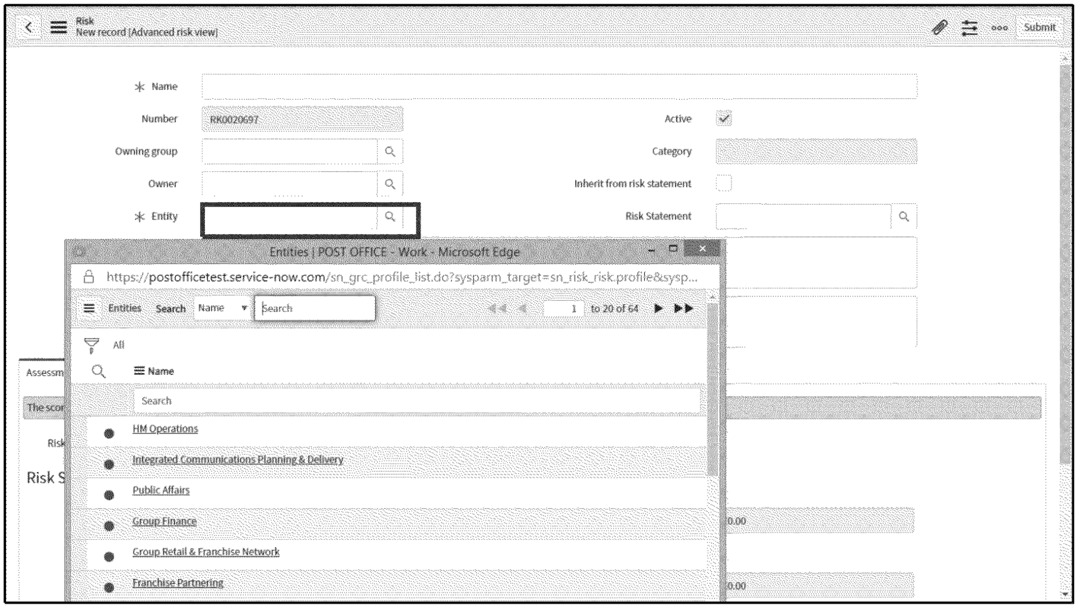
ServiceNow
Risk Management User Guide

POST OFFICE

1 RISK MANAGEMENT OVERVIEW

1.1 ENTITIES

- Post Office has a three-level risk hierarchy: Enterprise Risks (the Post Office's key business risks), Intermediate Risks (sub-categories of an enterprise risk to which they are linked) and Local Risks (sub-categories of intermediate risks, to which they are linked).
- Entities in ServiceNow (SNOW) mirror the Post Office three-level risk hierarchy.
- Entity field is visible in the Risk record (refer to paragraph 2.4.2 for details on how to complete a risk record).



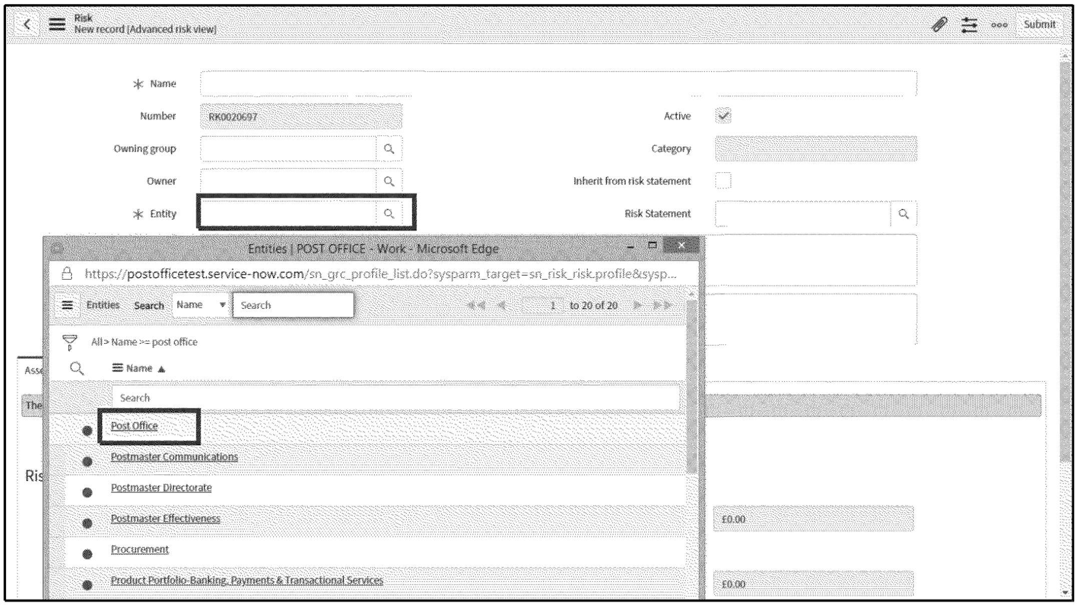
Name
Number RK0020697
Active ✓
Owning group
Category
Owner
Inherit from risk statement □
Entity
Risk Statement

Entities | POST OFFICE - Work - Microsoft Edge
https://postofficetest.service-now.com/sn_grc_profile_list.do?sysparm_target=sn_risk_risk.profile&sysp...

- HM Operations
- Integrated Communications Planning & Delivery
- Public Affairs
- Group Finance
- Group Retail & Franchise Network
- Franchise Partnering

Post Office Entity

- Post Office Entity refers to Enterprise Risks. These risks are Post Office-wide and so are of corporate importance. Each enterprise risk is owned by a relevant GE member. It is unlikely that Risk Users will need to select this Entity. Central Risk provide an update on the management of these enterprise risks at each RCC and ARC.


Risk
New record [Advanced risk view]

* Name
Number: RK0020697
Active: ☑
Owning group
Category
Owner
Inherit from risk statement: □
* Entity
Risk Statement

Entities | POST OFFICE - Work - Microsoft Edge
https://postofficetest.service-now.com/sn_grc_profile_list.do?sysparm_target=sn_risk_risk.profile&sysp...

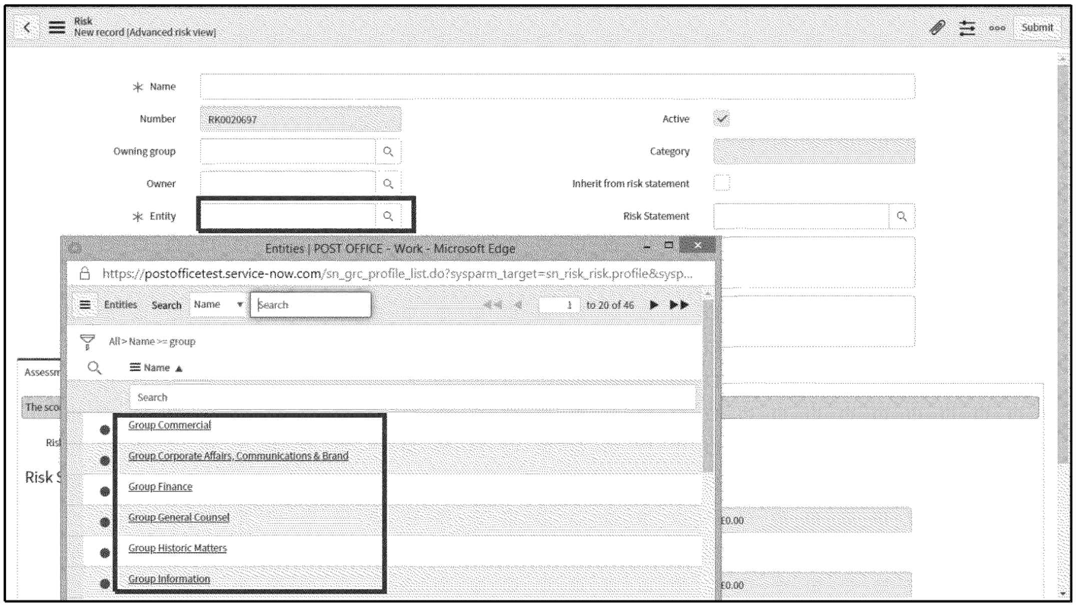
All > Name >= post office
Name ▲

- Post Office
- Postmaster Communications
- Postmaster Directorate
- Postmaster Effectiveness
- Procurement
- Product Portfolio-Banking, Payments & Transactional Services

£0.00
£0.00

Group Level Entity

- Entities that contain 'Group' refers to Intermediate Risks. They are often the key risks faced by individual business areas and they are often owned by GE/GE-1 member. Select these Entities only if the risk is relevant at GE /GE-1 member level (e.g. Group Commercial, Group Information, Group Finance etc).


Risk
New record [Advanced risk view]

* Name
Number: RK0020697
Active: ☑
Owning group
Category
Owner
Inherit from risk statement: □
* Entity
Risk Statement

Entities | POST OFFICE - Work - Microsoft Edge
https://postofficetest.service-now.com/sn_grc_profile_list.do?sysparm_target=sn_risk_risk.profile&sysp...

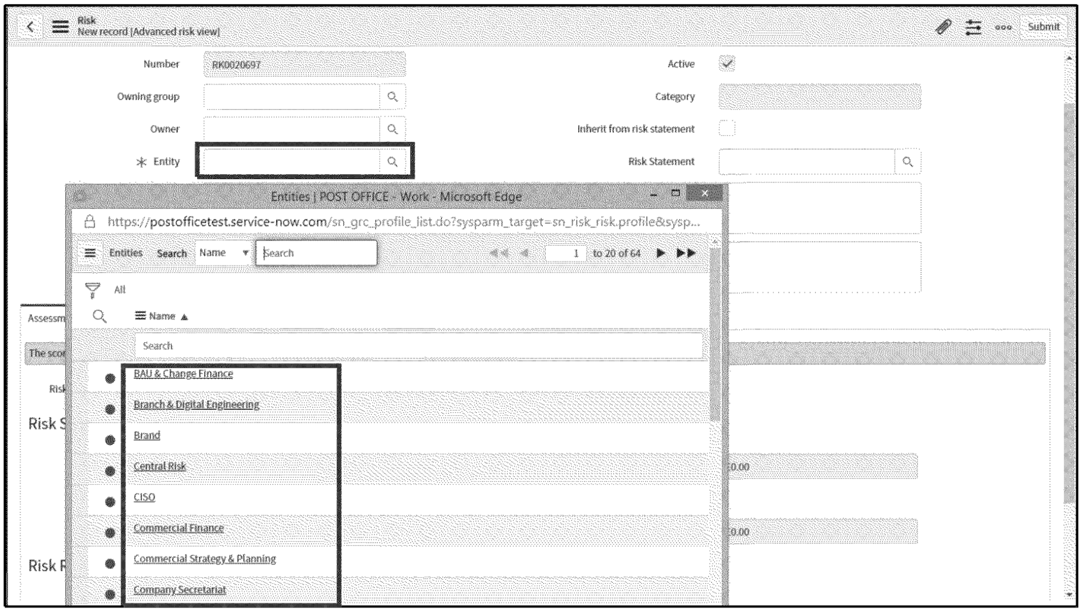
All > Name >= group
Name ▲

- Group Commercial
- Group Corporate Affairs, Communications & Brand
- Group Finance
- Group General Counsel
- Group Historic Matters
- Group Information

£0.00
£0.00

All other Entities

- All other Entities are related to Local Risks (Department level). They are often more specific, local risks faced by individual department and often owned by Department heads. Select these Entities only if risks are relevant at Department level.



Risk
New record [Advanced risk view]

Number RK0020697

Active ☑

Owning group

Category

Owner

Inherit from risk statement □

✱ Entity

Risk Statement

Entities | POST OFFICE - Work - Microsoft Edge

https://postofficetest.service-now.com/sn_grc_profile_list.do?sysparm_target=sn_risk_risk.profile&sysp...

Entities Search Name Search 1 to 20 of 64

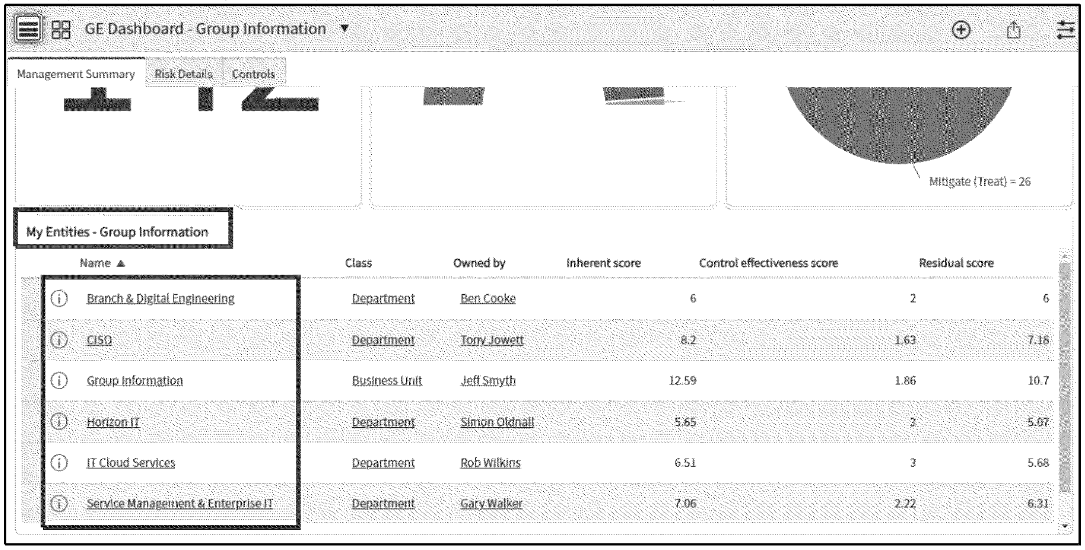
All

Name ▲

Search

- BAU & Change Finance
- Branch & Digital Engineering
- Brand
- Central Risk
- CISO
- Commercial Finance
- Commercial Strategy & Planning
- Company Secretariat

- If you are an Entity owner, you can see the entities you own under your GE Dashboard.



GE Dashboard - Group Information

My Entities - Group Information

Name ▲	Class	Owned by	Inherent score	Control effectiveness score	Residual score
Branch & Digital Engineering	Department	Ben Cooke	6	2	6
CISO	Department	Tony Jowett	8.2	1.63	7.18
Group Information	Business Unit	Jeff Smyth	12.59	1.86	10.7
Horizon IT	Department	Simon Oldnall	5.65	3	5.07
IT Cloud Services	Department	Rob Wilkins	6.51	3	5.68
Service Management & Enterprise IT	Department	Gary Walker	7.06	2.22	6.31

1.2 UPSTREAM AND DOWNSTREAM RISKS

- Risk hierarchy is managed by Central Risk Team linking Local risks to their related Intermediate risks and then to the related Enterprise risk, within the same Entity only. In SNOW this can be done linking your risk to Upstream and Downstream risks, depending on the risk level (e.g. if you have an intermediate risk, its upstream risk will be an Enterprise risk and downstream risk a Local risk).
- If you wish to change the risk hierarchy by adding/removing Upstream or Downstream risks, contact your Central Risk Business Partner (RBP) by ServiceNow chatbox message/email.

1.3 RISK STATEMENTS

- Risk Statements in SNOW are the Risk categories. Risk Statements can only be assigned by Central Risk Team.
- Each risk needs to be associated to a Risk Statement. There are more than55 Risk Statements 2 (sub-categories) across the 14 Risk Statement 1 (main categories).

Risk statement 1 in ServiceNow					
1	Strategy	**6**	Financial	**11**	Security
2	Governance	**7**	Commercial	**12**	Change
3	Operational	**8**	People	**13**	Reputational
4	Legal	**9**	Technology	**14**	Marketplace & Brands
5	Health & Safety	**10**	Information		

- Risks should be classified against the Event not the Cause or the Impact.
- ServiceNow risks management has enabled the Central Risk Team to view the risks not only by Group Entity (the verticals) but risk management across risk functions (technology, security, information) to address risk domains.

1.4 RISK OWNER

- ISO Guide 73 defines risk owner as a 'person with authority and accountability to make the decision to treat, or not to treat a risk'.
- Under the "first line of defence", management have primary ownership, responsibility and accountability for identifying, assessing and managing risks. The first line 'own' the risks and are responsible for execution of the organisation's response to those risks through executing internal controls on a day-to-day basis and for implementing corrective actions to address deficiencies.

1.5 RISK DESCRIPTION

- Risks must be expressed in terms of their cause(s), the risk event itself, and their impact:
  - Cause: A cause is an element which alone or in combination with other causes has the potential to give rise to the risk.
  - Event: An event is an articulation of the potential adverse or beneficial circumstances that could result from the cause – in effect the risk itself.
  - Consequences/Impact: Consequences are the outcome of a risk event materialising. Outcomes can be positive or negative.

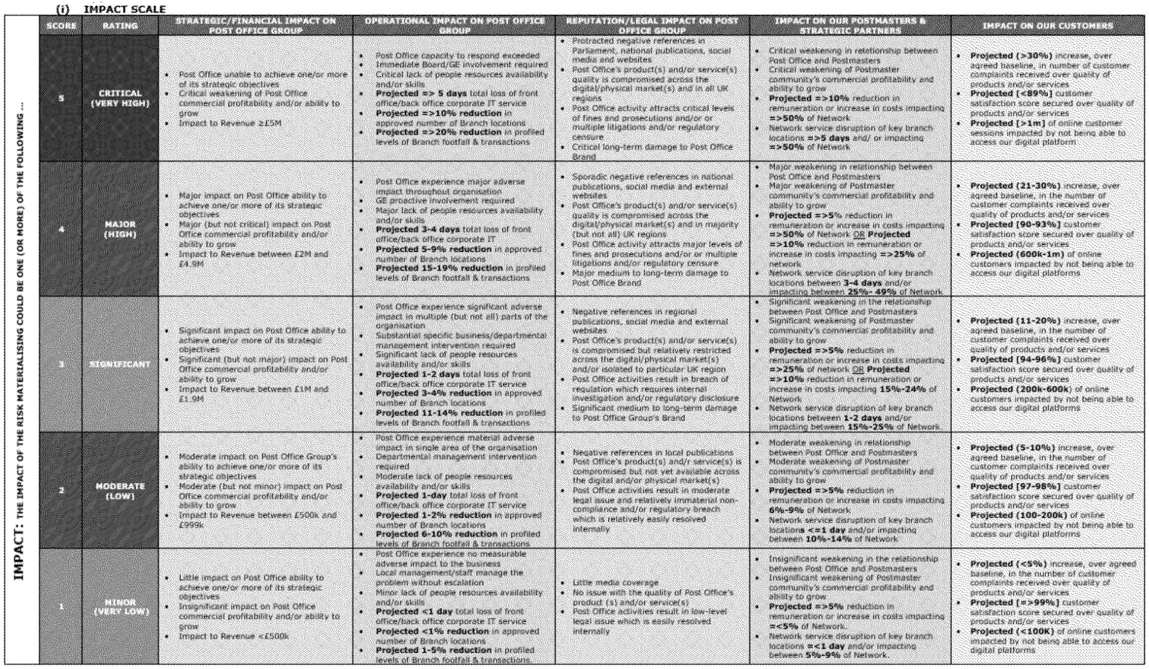
  A good example of risk description is as follows:

Cause	Event	Impact
Because of the lack of engagement, approach and transparency with the CWU members,	*there is a risk the Post Office experiences prolonged industrial action which adversely impacts its ability to deliver its short, medium or long-term strategic objectives,*	*resulting loss in revenue, client/customer detriment and reputational damage.*

1.6 POST OFFICE HARM TABLE

- A risk is assessed on both the likelihood of it occurring and the impact if it were to occur.
- The Post Office corporate HARM table (see table below) describes the likelihood/impact scales which must be applied, as per below:
  - likelihood score (between 1 and 5) indicates how probable it is that your risk is going to occur.
  - expected impact score (between 1 and 5): impact of your risk in any relevant impact category (i.e. Strategic/Financial, Operational, Reputational/Legal, Postmasters and Customers). The highest number (between 1 and 5) out of all the categories is the impact score for your risk and the category in which this occurs is the 'leading risk impact'.
  - Impact and likelihood are multiplied together to give the risk score (a minimum of 1 and a maximum of 25).

(i) IMPACT SCALE



	SCORE	RATING	STRATEGIC/FINANCIAL IMPACT ON POST OFFICE GROUP	OPERATIONAL IMPACT ON POST OFFICE GROUP	REPUTATION/LEGAL IMPACT ON POST OFFICE GROUP	IMPACT ON OUR POSTMASTERS & STRATEGIC PARTNERS	IMPACT ON OUR CUSTOMERS
IMPACT: THE IMPACT OF THE RISK MATERIALISING COULD BE ONE (OR MORE) OF THE FOLLOWING …	5	CRITICAL (VERY HIGH)	• Post Office unable to achieve one/or more of its strategic objectives • Critical weakening of Post Office commercial profitability and/or ability to grow • Impact to Revenue ≥£5M	• Post Office capacity to respond exceeded • Immediate Board/GE involvement required • Critical lack of people resources availability and/or skills • **Projected => 5 days** total loss of front office/back office corporate IT service • **Projected =>10% reduction** in approved number of Branch locations • **Projected =>20% reduction** in profiled levels of Branch footfall & transactions	• Protracted negative references in Parliament, national publications, social media and websites • Post Office's product(s) and/or service(s) quality is compromised across the digital/physical market(s) and in all UK regions • Post Office activity attracts critical levels of fines and prosecutions and/or or multiple litigations and/or regulatory censure • Critical long-term damage to Post Office Brand	• Critical weakening in relationship between Post Office and Postmasters • Critical weakening of Postmaster community's commercial profitability and ability to grow • **Projected =>10%** reduction in remuneration or increase in costs impacting **=>50%** of Network • Network service disruption of key branch locations **=>5 days** and/ or impacting **=>50%** of Network	• **Projected (>30%)** increase, over agreed baseline, in number of customer complaints received over quality of products and/or services • **Projected [<89%]** customer satisfaction score secured over quality of products and/or services • **Projected [>1m]** of online customer sessions impacted by not being able to access our digital platform
	4	MAJOR (HIGH)	• Major impact on Post Office ability to achieve one/or more of its strategic objectives • Major (but not critical) impact on Post Office commercial profitability and/or ability to grow • Impact to Revenue between £2M and £4.9M	• Post Office experience major adverse impact throughout organisation • GE proactive involvement required • Major lack of people resources availability and/or skills • **Projected 3-4 days** total loss of front office/back office corporate IT • **Projected 5-9% reduction** in approved number of Branch locations • **Projected 15-19% reduction** in profiled levels of Branch footfall & transactions	• Sporadic negative references in national publications, social media and external websites • Post Office's product(s) and/or service(s) quality is compromised across the digital/physical market(s) and in majority (but not all) UK regions • Post Office activity attracts major levels of fines and prosecutions and/or or multiple litigations and/or regulatory censure • Major medium to long-term damage to Post Office Brand	• Major weakening in relationship between Post Office and Postmasters • Major weakening of Postmaster community's commercial profitability and ability to grow • **Projected =>5%** reduction in remuneration or increase in costs impacting **=>50%** of Network OR **Projected =>10%** reduction in remuneration or increase in costs impacting **=>25%** of network • Network service disruption of key branch locations between **3-4 days** and/or impacting between **25%- 49%** of Network	• **Projected (21-30%)** increase, over agreed baseline, in the number of customer complaints received over quality of products and/or services • **Projected [90-93%]** customer satisfaction score secured over quality of products and/or services • **Projected (600k-1m)** of online customers impacted by not being able to access our digital platforms
	3	SIGNIFICANT	• Significant impact on Post Office ability to achieve one/or more of its strategic objectives • Significant (but not major) impact on Post Office commercial profitability and/or ability to grow • Impact to Revenue between £1M and £1.9M	• Post Office experience significant adverse impact in multiple (but not all) parts of the organisation • Substantial specific business/departmental management intervention required • Significant lack of people resources availability and/or skills • **Projected 1-2 days** total loss of front office/back office corporate IT service • **Projected 3-4% reduction** in approved number of Branch locations • **Projected 11-14% reduction** in profiled levels of Branch footfall & transactions	• Negative references in regional publications, social media and external websites • Post Office's product(s) and/or service(s) is compromised but relatively restricted across the digital/physical market(s) and/or isolated to particular UK region • Post Office activities result in breach of regulation which requires internal investigation and/or regulatory disclosure • Significant medium to long-term damage to Post Office Group's Brand	• Significant weakening in the relationship between Post Office and Postmasters • Significant weakening of Postmaster community's commercial profitability and ability to grow • **Projected =>5%** reduction in remuneration or increase in costs impacting **=>25%** of network OR **Projected =>10%** reduction in remuneration or increase in costs impacting **15%-24%** of Network • Network service disruption of key branch locations between **1-2 days** and/or impacting between **15%-25%** of Network	• **Projected (11-20%)** increase, over agreed baseline, in the number of customer complaints received over quality of products and/or services • **Projected [94-96%]** customer satisfaction score secured over quality of products and/or services • **Projected (200k-600k)** of online customers impacted by not being able to access our digital platforms
	2	MODERATE (LOW)	• Moderate impact on Post Office Group's ability to achieve one/or more of its strategic objectives • Moderate (but not minor) impact on Post Office commercial profitability and/or ability to grow • Impact to Revenue between £500k and £999k	• Post Office experience material adverse impact in single area of the organisation • Departmental management intervention required • Moderate lack of people resources availability and/or skills • **Projected 1-day** total loss of front office/back office corporate IT service • **Projected 1-2% reduction** in approved number of Branch locations • **Projected 6-10% reduction** in profiled levels of Branch footfall & transactions	• Negative references in local publications • Post Office's product(s) and/r service(s) is compromised but not yet available across the digital and/or physical market(s) • Post Office activities result in moderate legal issue and relatively immaterial non-compliance and/or regulatory breach which is relatively easily resolved internally	• Moderate weakening in relationship between Post Office and Postmasters • Moderate weakening of Postmaster community's commercial profitability and ability to grow • **Projected =>5%** reduction in remuneration or increase in costs impacting **6%-9%** of Network • Network service disruption of key branch locations **<=1 day** and/or impacting between **10%-14%** of Network	• **Projected (5-10%)** increase, over agreed baseline, in the number of customer complaints received over quality of products and/or services • **Projected [97-98%]** customer satisfaction score secured over quality of products and/or services • **Projected (100-200k)** of online customers impacted by not being able to access our digital platforms
	1	MINOR (VERY LOW)	• Little impact on Post Office ability to achieve one/or more of its strategic objectives • Insignificant impact on Post Office commercial profitability and/or ability to grow • Impact to Revenue <£500k	• Post Office experience no measurable adverse impact to the business • Local management/staff manage the problem without escalation • Minor lack of people resources availability and/or skills • **Projected <1 day** total loss of front office/back office corporate IT service • **Projected <1% reduction** in approved number of Branch locations • **Projected 1-5% reduction** in profiled levels of Branch footfall & transactions.	• Little media coverage • No issue with the quality of Post Office's product (s) and/or service(s) • Post Office activities result in low-level legal issue which is easily resolved internally	• Insignificant weakening in the relationship between Post Office and Postmasters • Insignificant weakening of Postmaster community's commercial profitability and ability to grow • **Projected =>5%** reduction in remuneration or increase in costs impacting **=<5%** of Network. • Network service disruption of key branch locations **=<1 day** and/or impacting between **5%-9%** of Network.	• **Projected (<5%)** increase, over agreed baseline, in the number of customer complaints received over quality of products and/or services • **Projected [=>99%]** customer satisfaction score secured over quality of products and/or services • **Projected (<100K)** of online customers impacted by not being able to access our digital platforms

(i) LIKELIHOOD SCALE

	SCORE	RATING	DESCRIPTION
LIKELIHOOD: THE LIKELIHOOD OF RISK MATERIALISING	5	ALMOST CERTAIN/VERY HIGH	• Risk almost certain to materialise unless action taken • Risk could be expected to materialise
	4	LIKELY/HIGH	• Risk likely to materialise frequently if events follow normal patterns and mitigating action is not taken. • Risk could be expected to materialise
	3	POSSIBLE/MODERATE	• Risk unlikely to materialise but it is possible • Risk could be expected to materialise infrequently/irregularly/sporadically
	2	UNLIKELY/LOW	• Risk very unlikely to materialise • Risk could materialise intermittently
	1	RARE/VERY LOW	• A remote likelihood that risk would materialise • Almost inconceivable that risk would occur

- Each active risk has 2 ratings namely:
  - Inherent: the level of risk before any control activities are applied.
  - Residual: the latest level of risk considering the effectiveness of the controls currently in place.

- The residual score cannot be higher (and will almost certainly be lower than) the inherent score. It may be equal to the inherent score on a new risk with no controls or remediation activity in place, but you would expect to see the residual score gradually reduce over time as the risk is managed.

1.7 CONTROL ASSESSMENT SCORE

- Control is any action taken to reduce the likelihood and/or magnitude of a risk.
- You can use the following guidance when assessing your controls:

Control Effectiveness	**Performance**
Effective	The control(s) significantly reduces the risk, bringing the residual risk within appetite
Partially Effective	The control(s) has some impact on reducing the risk
Ineffective	The control(s) does not adequately address the risk

1.8 RISK RESPONSE TYPE

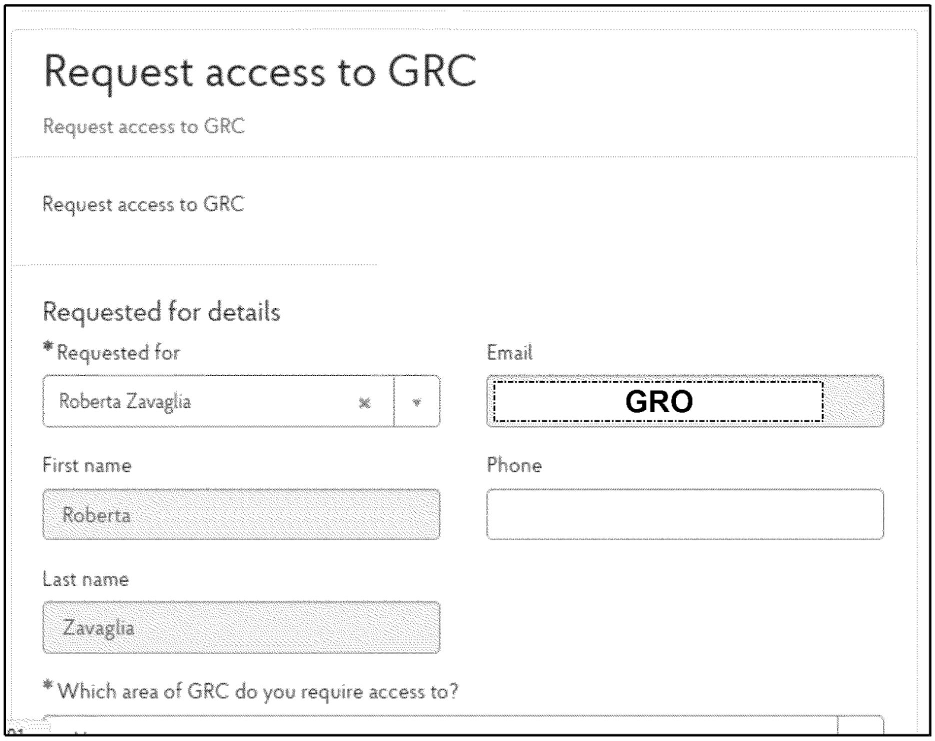
- You have the option for responding to risk, identified as the 4Ts: Accept (Tolerate), Mitigate (Treat), Transfer and Avoid (Terminate). Brief description of each of the 4Ts is provided below:

Risk Response	**Description**
Accept **(Tolerate/Retain)**	The risk exposure may be tolerable without any further action being taken. The ability to do anything about some risks may be limited, or the costs of taking any action may be disproportionate to the potential benefit gained.
Mitigate **(Treat/Control/Reduce)**	By far the greater number of risks will be addressed in this way. The purpose of treatment is that, whilst continuing within Post Office with the activity giving rise to the risk, mitigation plan is taken to constrain the risk within appetite
Transfer	Transferring a risk by means of an insurance policy (e.g. a cyber risk might be transferred because we have an insurance policy)
Avoid **(Terminate/Eliminate)**	Some risks will only be treatable or containable to acceptable levels, by terminating the activity. In these circumstances, appropriate responses will be elimination of the risk by stopping the process or activity, substituting an alternative process or outsourcing the activity that is associated with the risk (e.g., you can decide to ban the usage of laptops outside of the company premises if the risk of unauthorized access to those laptops is too high - because, e.g., such hacks could halt the complete IT infrastructure you are using)

2 HOW TO USE GRC SNOW

2.1 REQUEST ACCESS TO GRC SNOW

- If you require access to SNOW, you should fill a “Request access to GRC” form from SNOW Colleague Portal: Service Catalog - Colleague Portal (service-now.com)
- Contact your RBP if you have any issues or questions.



Request access to GRC

Request access to GRC

Request access to GRC

Requested for details

*Requested for: Roberta Zavaglia

Email: GRO

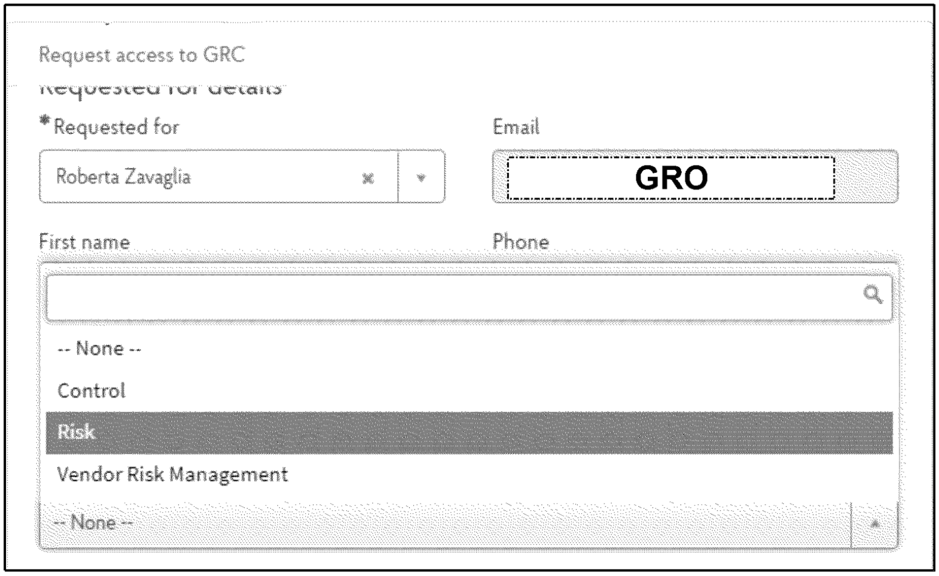
First name: Roberta

Phone:

Last name: Zavaglia

*Which area of GRC do you require access to?

- Select 'Risk' under 'Which area of GRC do you require access to?'



Request access to GRC

Requested for details

*Requested for: Roberta Zavaglia

Email: GRO

First name

Phone

-- None --

Control

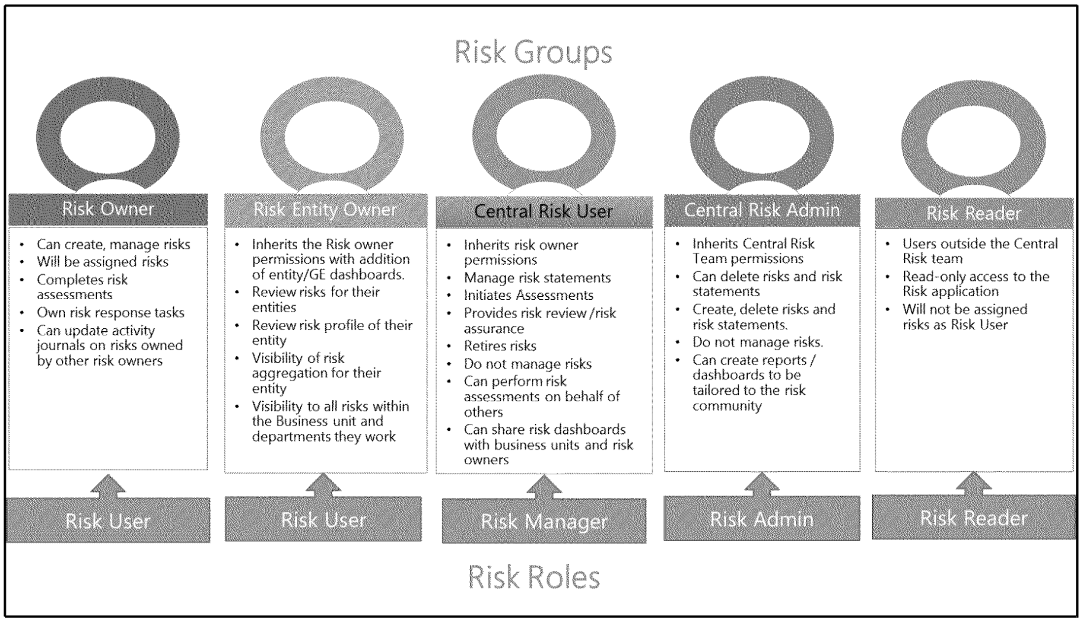
Risk

Vendor Risk Management

-- None --

- Select your Risk Group:
  - 'Risk Owner': if you own risks but you do not own anyDepartment or Business Unit (i.e. Entity);
  - 'Risk Entity Owner': if you are a risk owner and you own a Department or a Business Unit (i.e. Entity). You should be a GE or GE-1 member to request this Risk Group;
  - 'Central Risk Admin' and 'Central Risk User' are Risk groups for Central Risk Team only;

   - If you are not a risk owner but you need a read-only access to SNOW, speak to your RBP and ask how you can have 'Risk Reader' role. This Role cannot be requested through the Request access to GRC form.
- Each Risk Group is associate to a Risk Role and has the following abilities:



Risk Groups

Risk Owner
- Can create, manage risks
- Will be assigned risks
- Completes risk assessments
- Own risk response tasks
- Can update activity journals on risks owned by other risk owners

Risk User

Risk Entity Owner
- Inherits the Risk owner permissions with addition of entity/GE dashboards.
- Review risks for their entities
- Review risk profile of their entity
- Visibility of risk aggregation for their entity
- Visibility to all risks within the Business unit and departments they work

Risk User

Central Risk User
- Inherits risk owner permissions
- Manage risk statements
- Initiates Assessments
- Provides risk review /risk assurance
- Retires risks
- Do not manage risks
- Can perform risk assessments on behalf of others
- Can share risk dashboards with business units and risk owners

Risk Manager

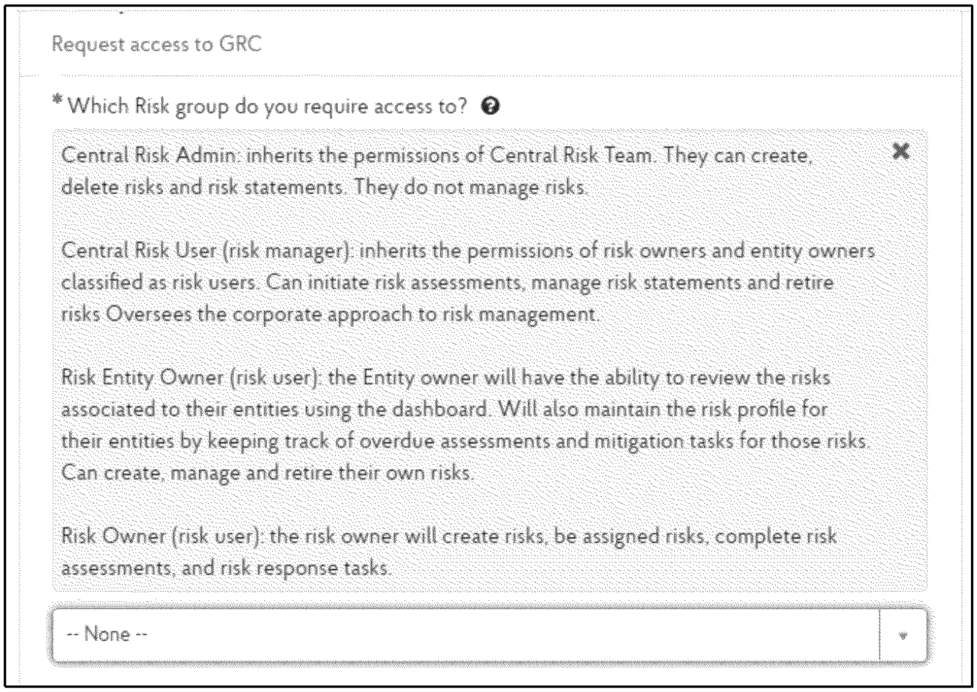
Central Risk Admin
- Inherits Central Risk Team permissions
- Can delete risks and risk statements
- Create, delete risks and risk statements.
- Do not manage risks.
- Can create reports / dashboards to be tailored to the risk community

Risk Admin

Risk Reader
- Users outside the Central Risk team
- Read-only access to the Risk application
- Will not be assigned risks as Risk User

Risk Reader

Risk Roles



Request access to GRC

* Which Risk group do you require access to?

Central Risk Admin: inherits the permissions of Central Risk Team. They can create, delete risks and risk statements. They do not manage risks.

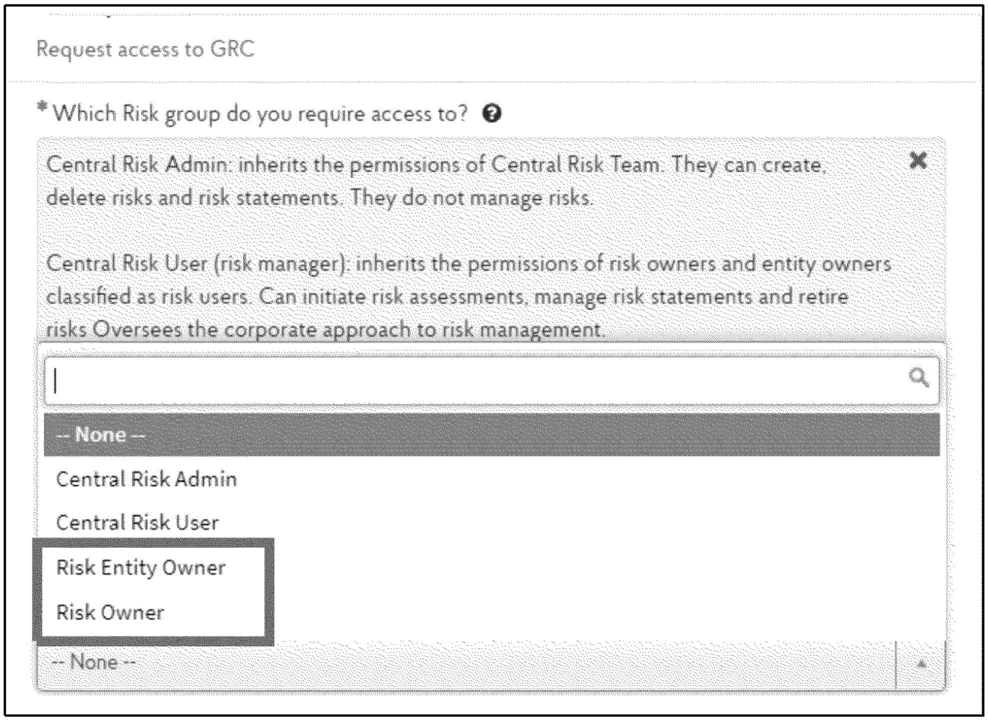
Central Risk User (risk manager): inherits the permissions of risk owners and entity owners classified as risk users. Can initiate risk assessments, manage risk statements and retire risks Oversees the corporate approach to risk management.

Risk Entity Owner (risk user): the Entity owner will have the ability to review the risks associated to their entities using the dashboard. Will also maintain the risk profile for their entities by keeping track of overdue assessments and mitigation tasks for those risks. Can create, manage and retire their own risks.

Risk Owner (risk user): the risk owner will create risks, be assigned risks, complete risk assessments, and risk response tasks.

-- None --

- Select either 'Risk Owner' or 'Risk Entity Owner' as 'Central Risk Admin' and 'Central Risk User' are for Central Risk Team only.



Request access to GRC

* Which Risk group do you require access to?

Central Risk Admin: inherits the permissions of Central Risk Team. They can create, delete risks and risk statements. They do not manage risks.

Central Risk User (risk manager): inherits the permissions of risk owners and entity owners classified as risk users. Can initiate risk assessments, manage risk statements and retire risks Oversees the corporate approach to risk management.

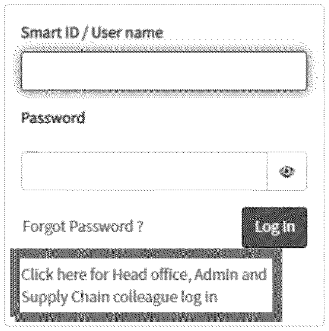
-- None --
Central Risk Admin
Central Risk User
Risk Entity Owner
Risk Owner

-- None --

- Your request of access will have to approved by your RBP.

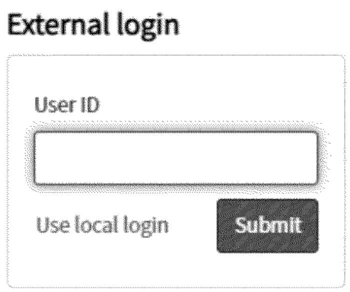
2.2 LOGIN INTO SNOW

- Once you have received access to SNOW, login into the system (you will login with your Post Office credentials)
- If you see the following screen select “Click here for Head Office, Admin and Supply Chain colleague log in”


Smart ID / User name
Password
Forgot Password ?
Log in
Click here for Head office, Admin and Supply Chain colleague log in

- Insert your email and you will login into SNOW

POL00447891



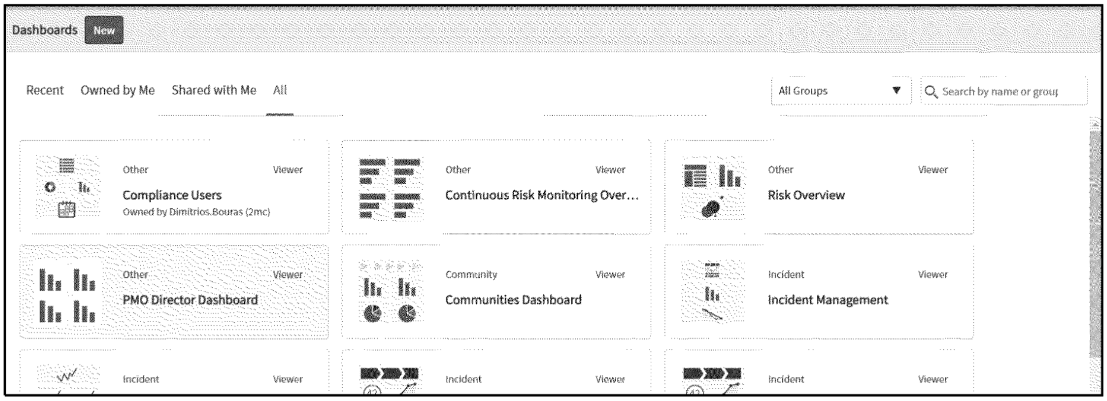
External login

User ID

Use local login

2.3 DEFAULT HOMEPAGE

- The first time you login you should see your Homepage set as Dashboards, as per screenshot below:



Other Viewer
Compliance Users
Owned by Dimitrios.Bouras (2mc)

Other Viewer
Continuous Risk Monitoring Over…

Other Viewer
Risk Overview

Other Viewer
PMO Director Dashboard

Community Viewer
Communities Dashboard

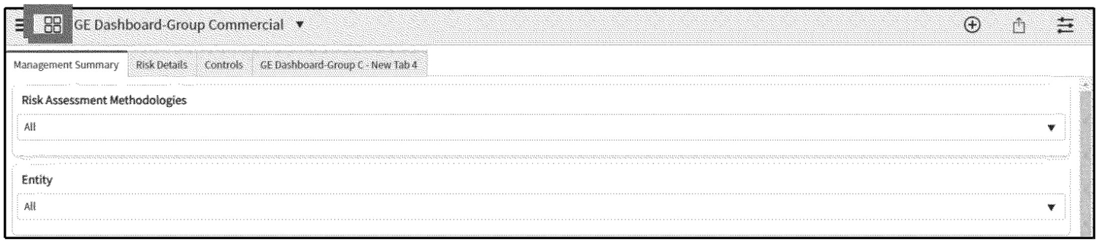
Incident Viewer
Incident Management

Incident Viewer

Incident Viewer

Incident Viewer

  - If not, click on the Dashboard overview icon as per below and you will be redirected to the interface above.

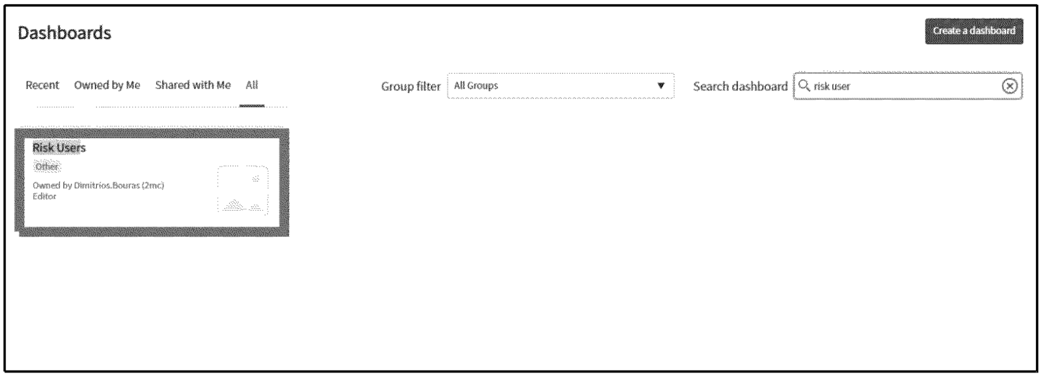


GE Dashboard-Group Commercial
Management Summary
Risk Details
Controls
GE Dashboard-Group C - New Tab 4

Risk Assessment Methodologies
All

Entity
All

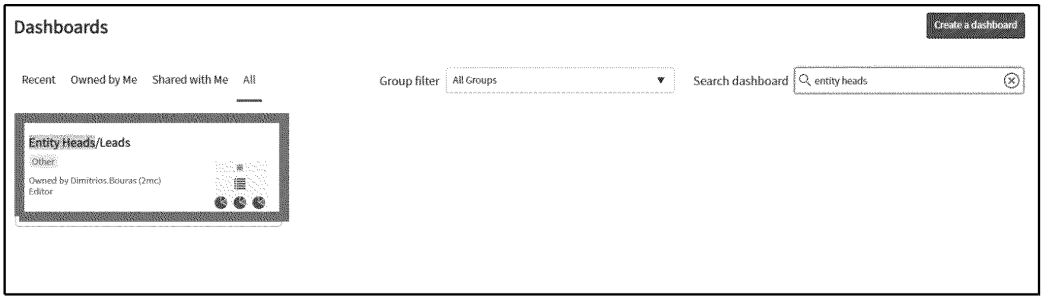
  - Select ‘All’ and type the Dashboard that you want to set up as a default in the Search Box:
    - “Risks Users” Dashboard: if you are a risk owner and you do not own any Department or Business Unit. This will give you visibility of the risks that you own;
    - “Entity Heads/Leads” Dashboard: if you are a risk owner and you own a Department or a Business Unit (i.e. Entity Owner), you can also select this dashboard. This will give you visibility of your Entities risks;
    - “GE Group” Dashboard (i.e. GE Group Commercial, Finance, Information, People etc.): if you are a risk owner and you own a Department or a Business Unit (i.e. Entity Owner), select the GE Group dashboard related to your Business Unit. This will give you visibility of your Business Unit Risk profile, Entity risks, outstanding risk assessments mitigation tasks, etc.



Group filter: All Groups

Search dashboard: risk user

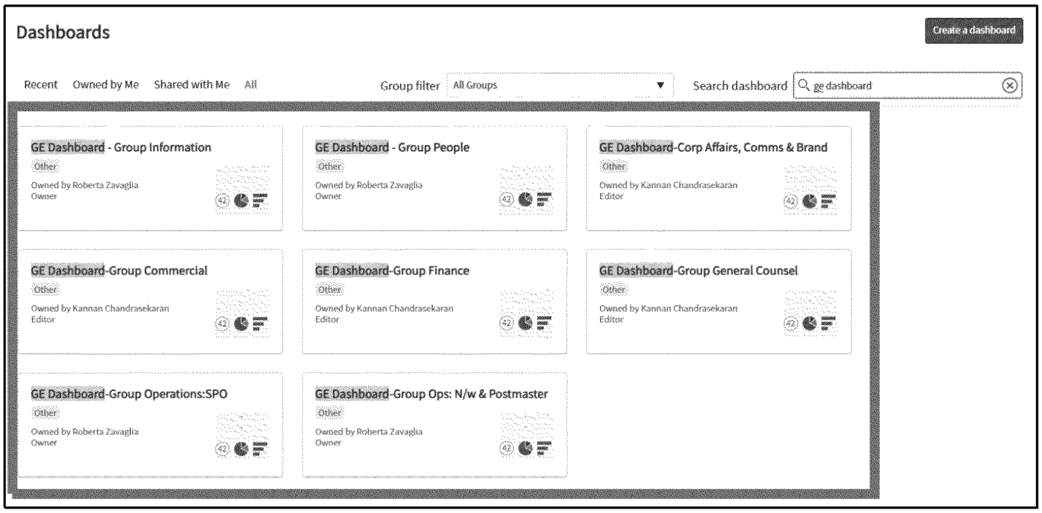
Risk Users
Other
Owned by Dimitrios.Bouras (2mc)
Editor



Group filter: All Groups

Search dashboard: entity heads

Entity Heads/Leads
Other
Owned by Dimitrios.Bouras (2mc)
Editor

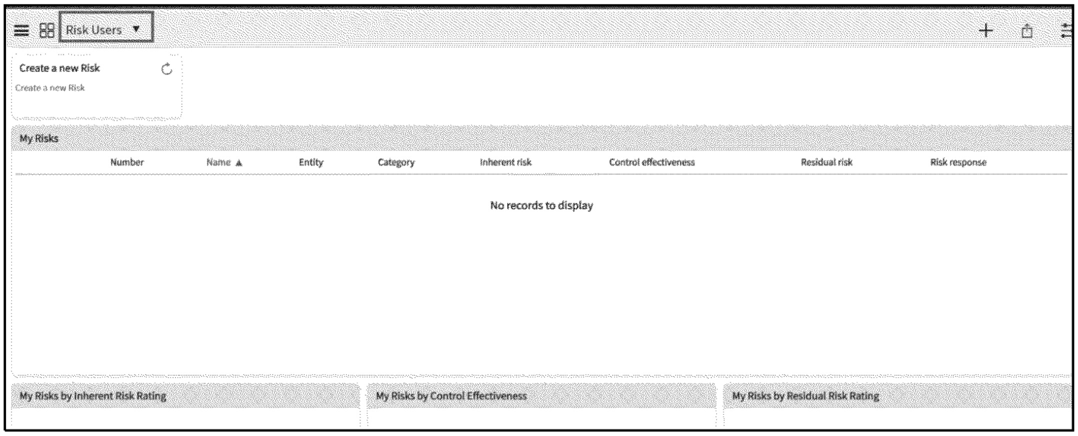


Group filter: All Groups

Search dashboard: ge dashboard

GE Dashboard - Group Information Other Owned by Roberta Zavaglia Owner	GE Dashboard - Group People Other Owned by Roberta Zavaglia Owner	GE Dashboard-Corp Affairs, Comms & Brand Other Owned by Kannan Chandrasekaran Editor
GE Dashboard-Group Commercial Other Owned by Kannan Chandrasekaran Editor	GE Dashboard-Group Finance Other Owned by Kannan Chandrasekaran Editor	GE Dashboard-Group General Counsel Other Owned by Kannan Chandrasekaran Editor
GE Dashboard-Group Operations:SPO Other Owned by Roberta Zavaglia Owner	GE Dashboard-Group Ops: N/w & Postmaster Other Owned by Roberta Zavaglia Owner	

- You will be redirected to the ‘Risk Users’ or your selected Dashboard. When you login ServiceNow and when you click on the top left corner (i.e. HomePage icon) you should always be redirected to the‘Risk Users’ Dashboard or your selected Dashboard.


Risk Users
Create a new Risk
Create a new Risk
My Risks
My Risks by Inherent Risk Rating
My Risks by Control Effectiveness
My Risks by Residual Risk Rating

Number	Name ▲	Entity	Category	Inherent risk	Control effectiveness	Residual risk	Risk response

No records to display

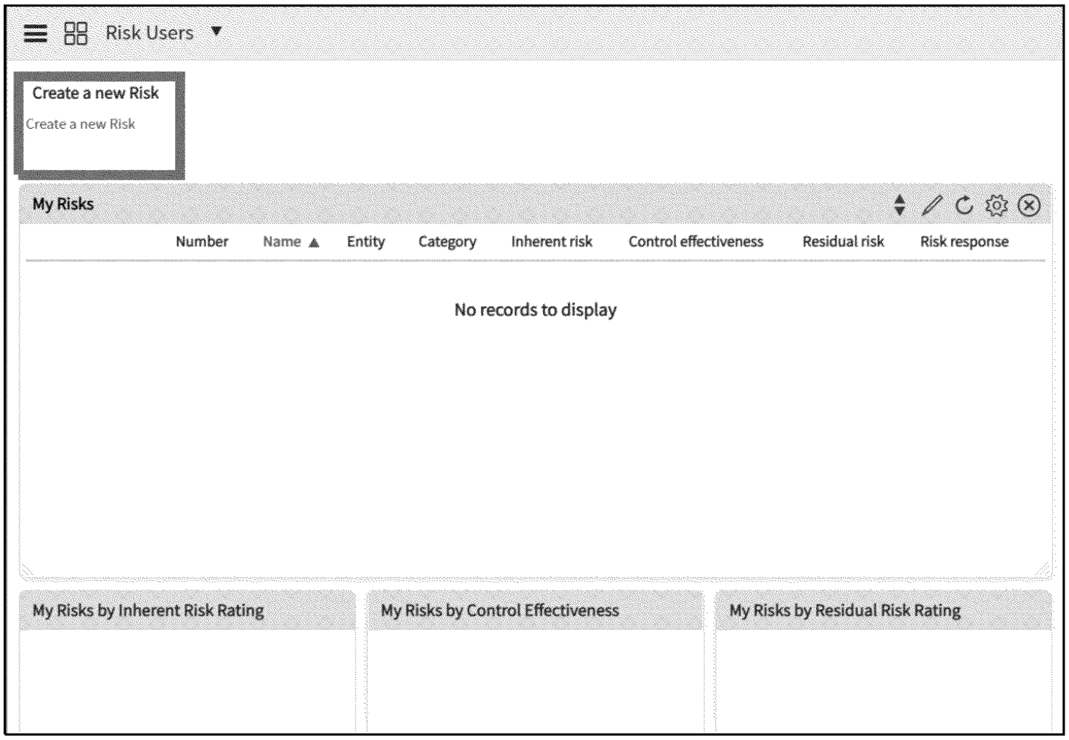
2.4 CREATE A NEW RISK

2.4.1 How to create a risk

- Risks are created by risk owners directly in the Risk application. There are several ways to do this:

OPTION 1: RISK USERS DASHBOARD

- The preferred method to create a new Risk is through yourRisk User Dashboard by clicking 'Create a new Risk' button.

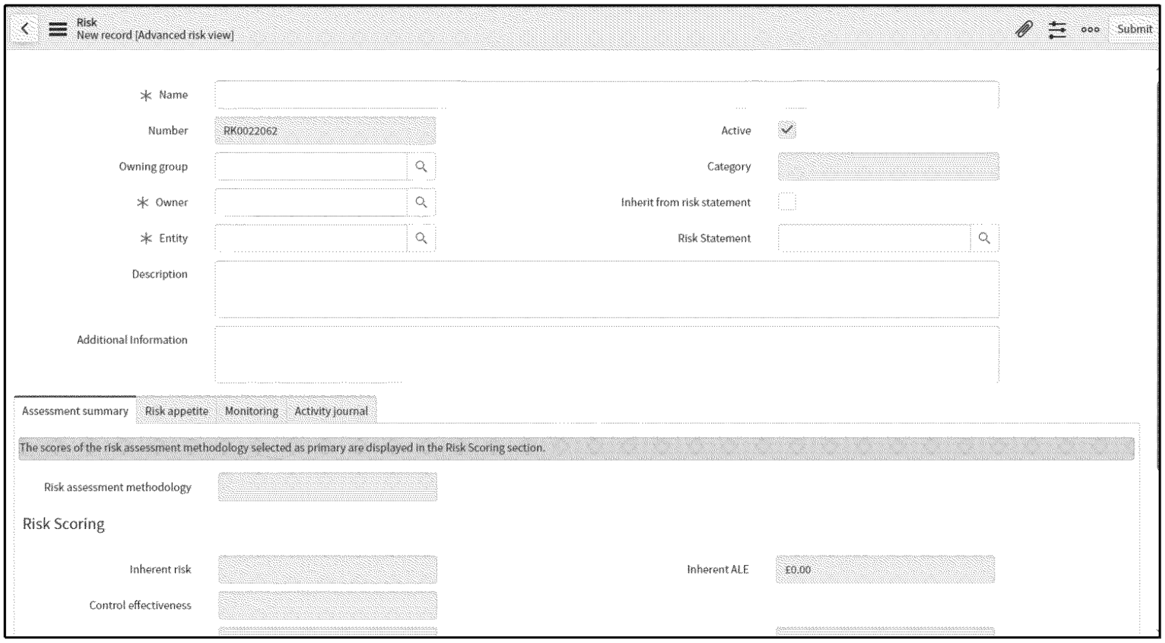

Risk Users
Create a new Risk
Create a new Risk
My Risks
My Risks by Inherent Risk Rating
My Risks by Control Effectiveness
My Risks by Residual Risk Rating

Number	Name ▲	Entity	Category	Inherent risk	Control effectiveness	Residual risk	Risk response

No records to display

POL00447891

- You will be redirected to the following page, where you can fill out and save the details of therisk (refer to paragraph 2.4.2 for details).



* Name			
Number	RK0022062	Active	☑
Owning group		Category	
* Owner		Inherit from risk statement	□
* Entity		Risk Statement	
Description			
Additional Information			

The scores of the risk assessment methodology selected as primary are displayed in the Risk Scoring section.

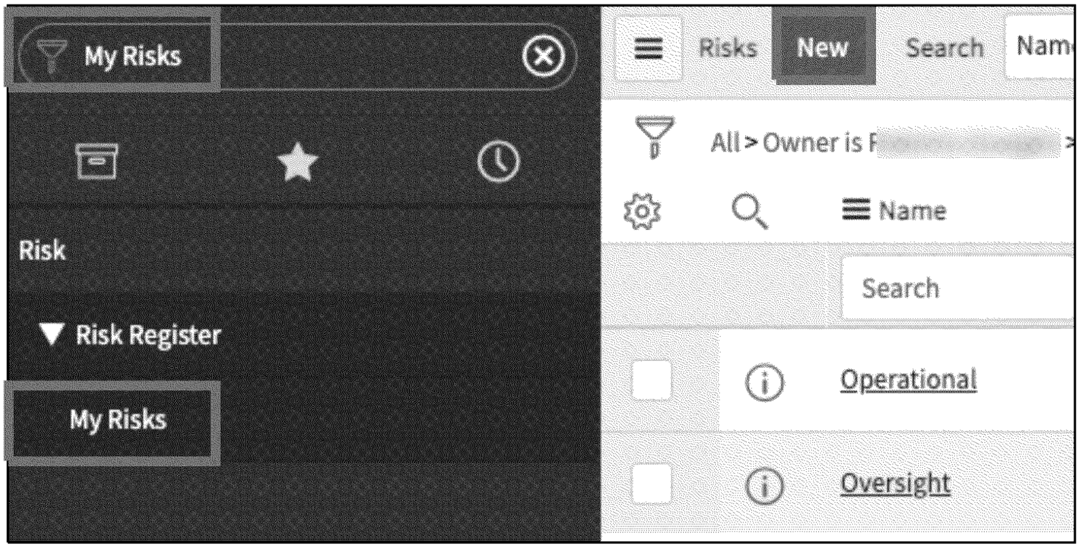
Risk assessment methodology

Risk Scoring

Inherent risk		Inherent ALE	£0.00
Control effectiveness			

OPTION 2: USING THE RISK APPLICATION

- Write ‘My Risks’ on the Filter navigator on the top left, click on ‘My Risks’ under Risk Register to display a list of all risks where you are a risk owner and click “New” button to create a new risk record:



All > Owner is F[redacted] >

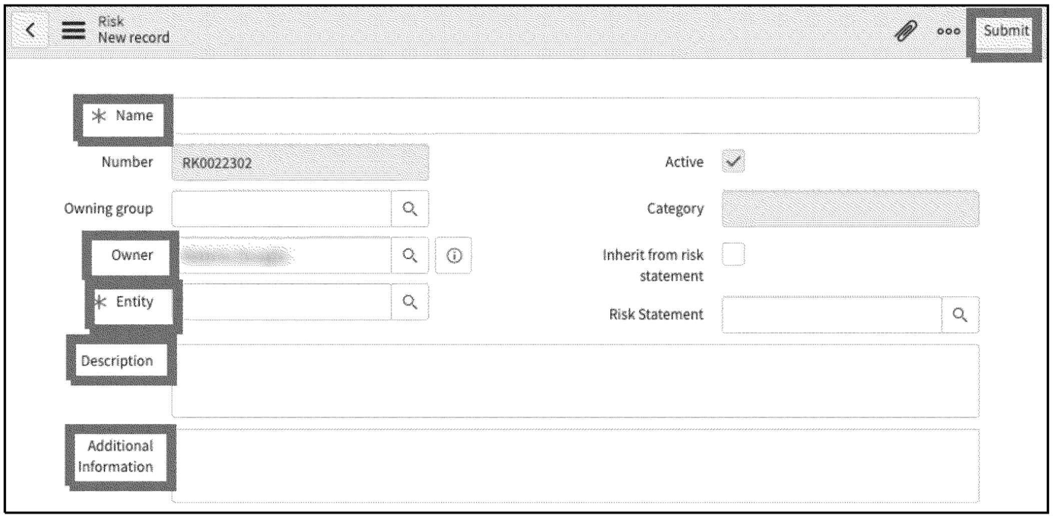
Operational

Oversight

POL00447891

2.4.2 Complete a risk record

- The following fields must be completed when you create a newrisk:
  - Name (mandatory) - short description of the risk.
  - Risk Owner (mandatory) - person with authority and accountability to make the decision to treat, or not to treat a risk (refer to paragraph 1.4 for definition).
  - Entity (mandatory) - mirrors the Post Office three-level risk hierarchy (Post Office/Enterprise risks, Group level/Intermediate risks, Department level/Local risks) - (refer to paragraph 1.1 for details).
  - Description (mandatory) - risks must be expressed in terms of their cause(s), the risk event itself, and their impact (refer to paragraph 1.5 for guidance).
  - Owning group field is not in use.
  - Risk Statements are the Risk categories and can only be assigned by Central Risk Team (refer to paragraph 1.3 for details).
  - Additional Information (not mandatory) can be used to add additional comments on your risk (e.g. comments on the reason why this risk has materialised, if this is because of a change of regulation or from an incident that occurred, what policies apply, Internal Audit findings, etc.).
- Select 'Submit' button on the top right to save the record and return to the previous screen.



Number: RK0022302

Active: ☑

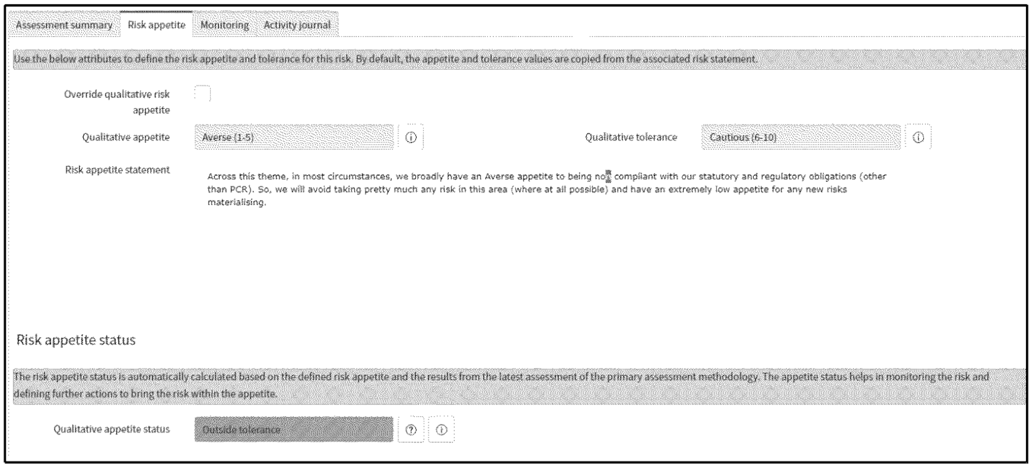
Owner: [redacted]

- The Central Risk Team then reviews the risk and associates the risk to the appropriate risk statement, before releasing the risk assessment.

2.4.3 Risk Appetite

- There is a Risk appetite tab under your risk record and risk assessment record showing the Risk Appetite and Tolerance levels linked to the Risk Statement of your risk (see screenshot below). POL has approved risk appetite and tolerance levels for the following areas: Technology, People, Commercial, Legal, Operational, Governance and Finance. If there is not an approved risk appetite statement, the risk appetite tab will be empty.
- Within the same tab, you can also see the risk appetite status, if the risk has been assessed before (the field will be empty if the risk has not been assessed yet). This shows if the risk is "inside appetite", "outside appetite" or "outside tolerance". You have to consider the risk appetite and tolerance when assessing your risk and completing the risk response (please see sections 2.6.6 and 2.6.7).

POL00447891



Use the below attributes to define the risk appetite and tolerance for this risk. By default, the appetite and tolerance values are copied from the associated risk statement.

Override qualitative risk appetite □

Qualitative appetite: Averse (1-5)

Qualitative tolerance: Cautious (6-10)

Risk appetite statement: Across this theme, in most circumstances, we broadly have an Averse appetite to being not compliant with our statutory and regulatory obligations (other than PCR). So, we will avoid taking pretty much any risk in this area (where at all possible) and have an extremely low appetite for any new risks materialising.

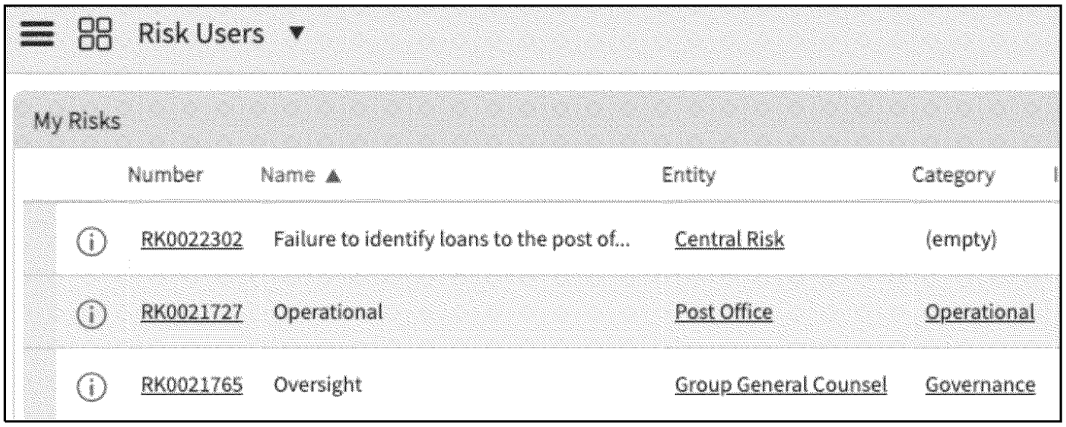
Risk appetite status

The risk appetite status is automatically calculated based on the defined risk appetite and the results from the latest assessment of the primary assessment methodology. The appetite status helps in monitoring the risk and defining further actions to bring the risk within the appetite.

Qualitative appetite status: Outside tolerance

2.5 LOCATE RISKS

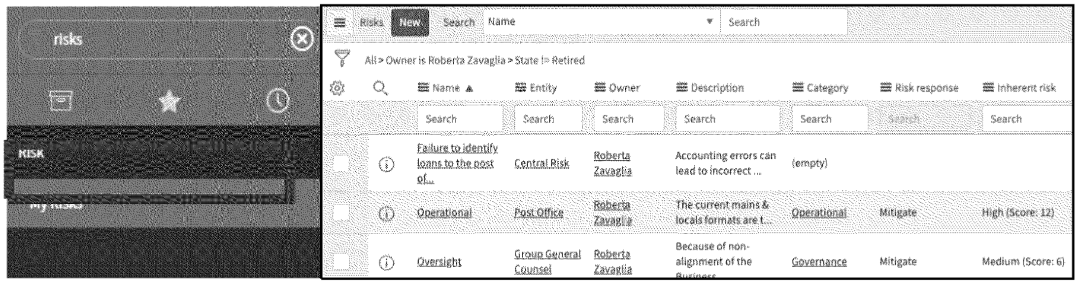
- The preferred method to locate your risks is through 'My Risks' section on your Risk Users Dashboard:



My Risks

Number	Name ▲	Entity	Category
RK0022302	Failure to identify loans to the post of...	Central Risk	(empty)
RK0021727	Operational	Post Office	Operational
RK0021765	Oversight	Group General Counsel	Governance

- Alternatively, you can select "risks' under Risk on the left panel, which shows all active risks of which you are the risk owner:

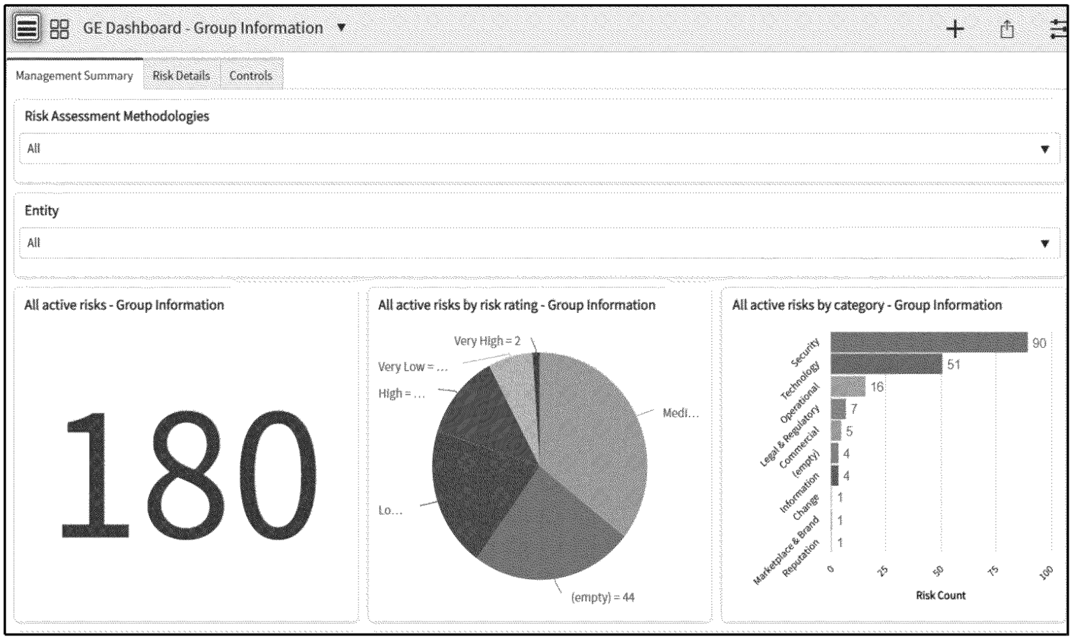


All > Owner is Roberta Zavaglia > State != Retired

Name ▲	Entity	Owner	Description	Category	Risk response	Inherent risk
Failure to identify loans to the post of...	Central Risk	Roberta Zavaglia	Accounting errors can lead to incorrect ...	(empty)		
Operational	Post Office	Roberta Zavaglia	The current mains & locals formats are t...	Operational	Mitigate	High (Score: 12)
Oversight	Group General Counsel	Roberta Zavaglia	Because of non-alignment of the Business	Governance	Mitigate	Medium (Score: 6)

- If you own a Business Unit or Department, you can also locate your Business Area risks from your GE Dashboard by clicking on to 'All active risks' chart or 'Risk Details' tab.

POL00447891



GE Dashboard - Group Information ▼

Management Summary | Risk Details | Controls

Risk Assessment Methodologies: All ▼

Entity: All ▼

2.6 ASSESS A RISK

2.6.1 **Notifications**

- You will receive a notification at important points in the life cycle of the riskassessment:
    - When the risk assessment has been initiated. You will receive an email with a link to the assessment, asking you to perform a risk assessment before the due date.
    - When the risk assessment has been re-assigned to you from the risk owner.
    - When risk assessment is due.
    - When risk assessment is overdue (the Due date has passed).
    - When a risk response task is assigned to you.
    - When a risk mitigation is overdue.

2.6.2 **Initiate a risk assessment**

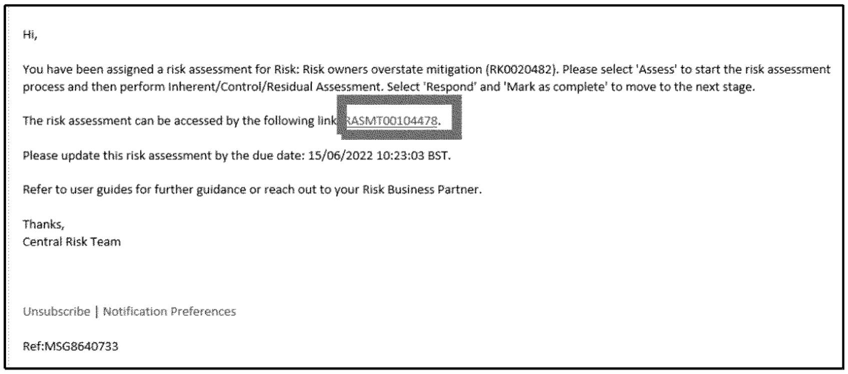
- You as a Risk Owner cannot initiate an assessment.
- All risks in a 'Mitigate' state will be released for assessment by the Central Risk Team driven by the dates aligned to RCC. SNOW Risk Assessment Schedule (including Risk assessment release dates and due dates for risk assessments to be completed) can be found in the Central Risk Team intranet page Governance, Risk & Compliance Tool (sharepoint.com).
- All risks in 'Accept' state will be automatically released for assessment by the system on the 'acceptance due date' (refer to paragraph 2.7.2 Risk Acceptance Task for more details).
- You can make ad hoc requests for risks that require assessments. In this case request to initiate an assessment to your RBP or Central Risk via risk chat or email:
    - If the risk in a Mitigate state has increased or decreased and you would urgently like to reflect this within the risk before the risk assessment release dates;
    - If you need to change a risk score before the acceptance due date;
    - If you have a new risk that has not been initiated;
    - If you wish to retire a risk (refer to paragraph 2.8)

POL00447891

- If you do not wish to change the scores before the risk assessment release dates, you add can detail to the activity journey to note for when you do assess the risk.

2.6.3 Start risk assessment process

- You should have received an email asking you to perform risk assessment, containing the link to the risk assessment to be performed:



Hi,

You have been assigned a risk assessment for Risk: Risk owners overstate mitigation (RK0020482). Please select 'Assess' to start the risk assessment process and then perform Inherent/Control/Residual Assessment. Select 'Respond' and 'Mark as complete' to move to the next stage.

The risk assessment can be accessed by the following link RASMT00104478.

Please update this risk assessment by the due date: 15/06/2022 10:23:03 BST.

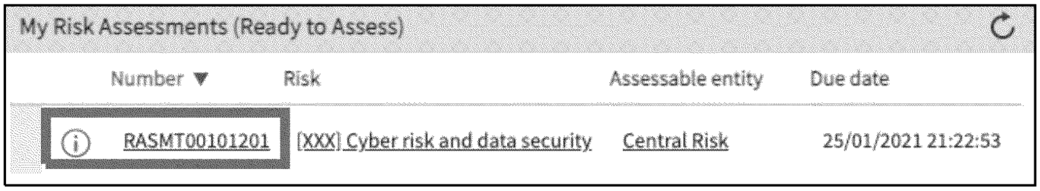
Refer to user guides for further guidance or reach out to your Risk Business Partner.

Thanks,
Central Risk Team

Unsubscribe | Notification Preferences

Ref:MSG8640733

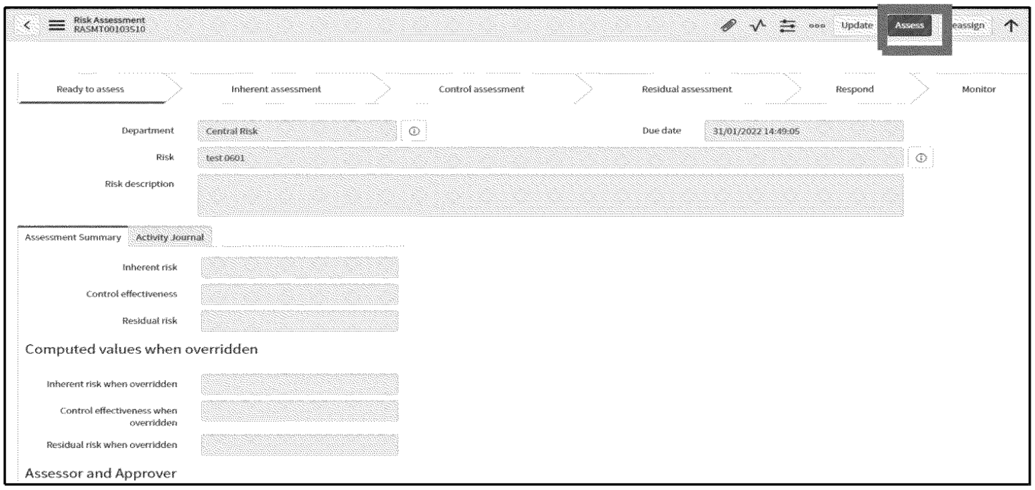
- Log into ServiceNow, load your Risk User dashboard and locate your risk assessments in "My Risk Assessments (Ready to Assess)" list in the middle of your dashboard. Working through one by one, click on the RASMT number (not the words).



My Risk Assessments (Ready to Assess)

Number ▼	Risk	Assessable entity	Due date
ⓘ RASMT00101201	[XXX] Cyber risk and data security	Central Risk	25/01/2021 21:22:53

- Click 'Assess' to start the risk assessment process to the inherent risk assessment. Always follow the green buttons at the top right hand of the page as these will move you through each stage of the risk assessment process.



Risk Assessment
RASMT00103510

Department: Central Risk
Due date: 31/01/2022 14:49:05
Risk: test 0601
Risk description:

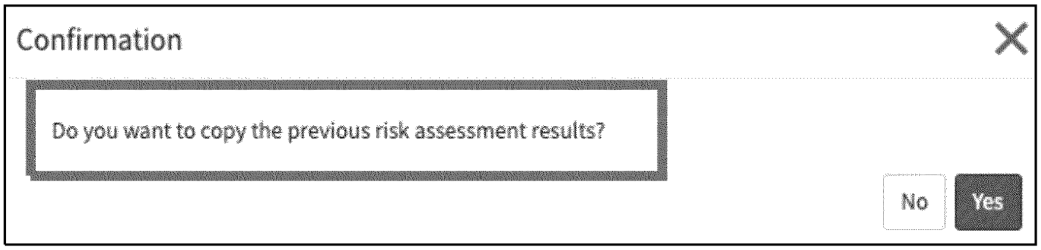
Inherent risk:
Control effectiveness:
Residual risk:

Computed values when overridden

Inherent risk when overridden:
Control effectiveness when overridden:
Residual risk when overridden:

Assessor and Approver

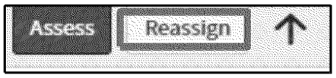
- If the risk was previously assessed, you will be asked if you want to bring forward the previous assessment. The preferred choice is 'Yes'.



Confirmation

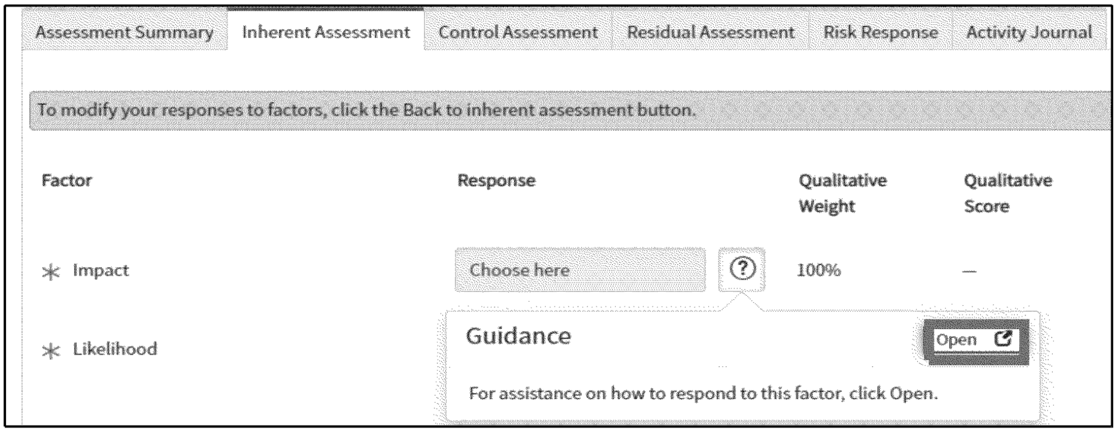
Do you want to copy the previous risk assessment results?

- You can click 'Reassign' in title bar to reassign assessment to another member of your team, in exceptional circumstances (e.g. long term sick):



2.6.4 Inherent Assessment

- The 1st stage of the risk assessment process is the 'Inherent Assessment'.
- The Inherent score is the level of risk before any control activities are applied.
- The Inherent score is determined when you assign likelihood and impact rating (between 1 and 5) to the risk. The Post Office corporate HARM table describes the impact/likelihood scales which must be applied and it can be viewed by clicking Open from the Guidance next to Impact/Likelihood(refer to paragraph 1.6 for details);



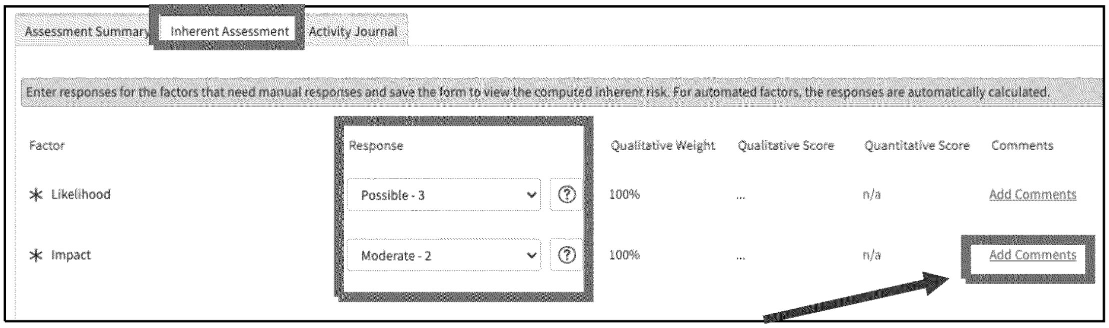
To modify your responses to factors, click the Back to inherent assessment button.

Factor	Response	Qualitative Weight	Qualitative Score
* Impact	Choose here	100%	–
* Likelihood			

Guidance

For assistance on how to respond to this factor, click Open.

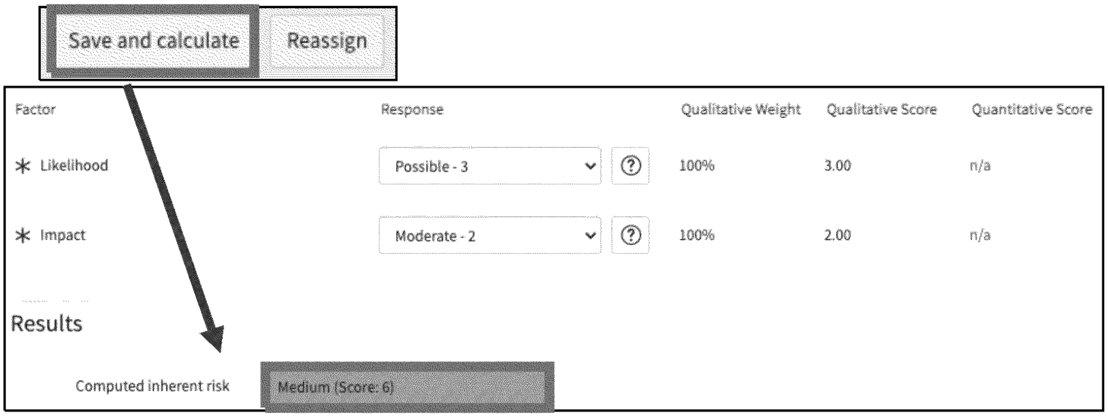
- For existing risks, the inherent score should not be amended, unless something material about the nature of the risk has changed. Ensure that the inherent score is either the same or higher than the residual score (not lower). For new risks with no controls or remediation activity in place, the inherent score may be equal to a residual score. If you make any changes to the inherent score, add your rationale in the comments box.



Enter responses for the factors that need manual responses and save the form to view the computed inherent risk. For automated factors, the responses are automatically calculated.

Factor	Response	Qualitative Weight	Qualitative Score	Quantitative Score	Comments
* Likelihood	Possible - 3	100%	...	n/a	Add Comments
* Impact	Moderate - 2	100%	...	n/a	Add Comments

- Click 'Save and calculate' at the top right hand of the page to calculate the risk score:

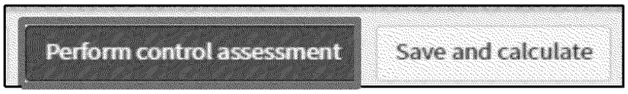


Factor	Response	Qualitative Weight	Qualitative Score	Quantitative Score
* Likelihood	Possible - 3	100%	3.00	n/a
* Impact	Moderate - 2	100%	2.00	n/a

Results

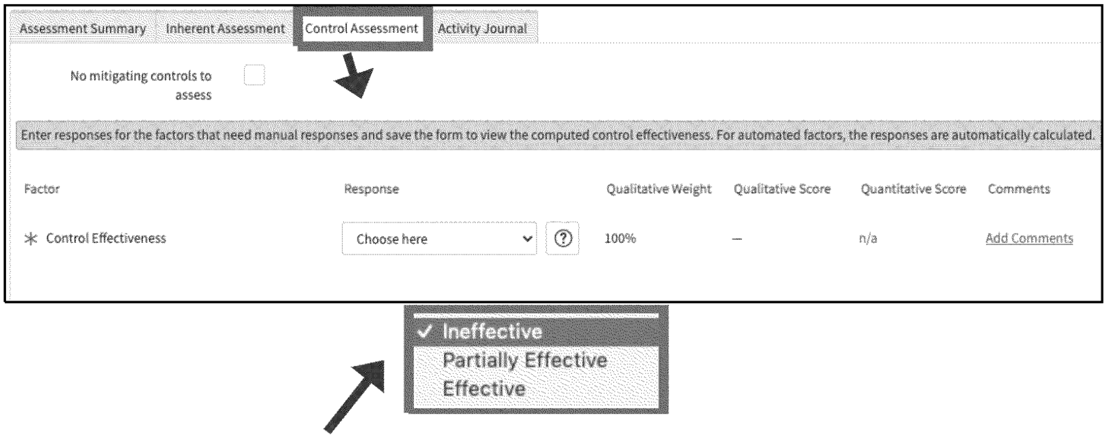
Computed inherent risk: Medium (Score: 6)

- Click 'Perform control assessment':



2.6.5 Control Assessment

- The 2nd stage of the risk assessment process is the 'Control assessment'.
- Select (tick) 'no mitigating controls to asses' if you are NOT live on the Controls Framework. Add your controls in the comment box.

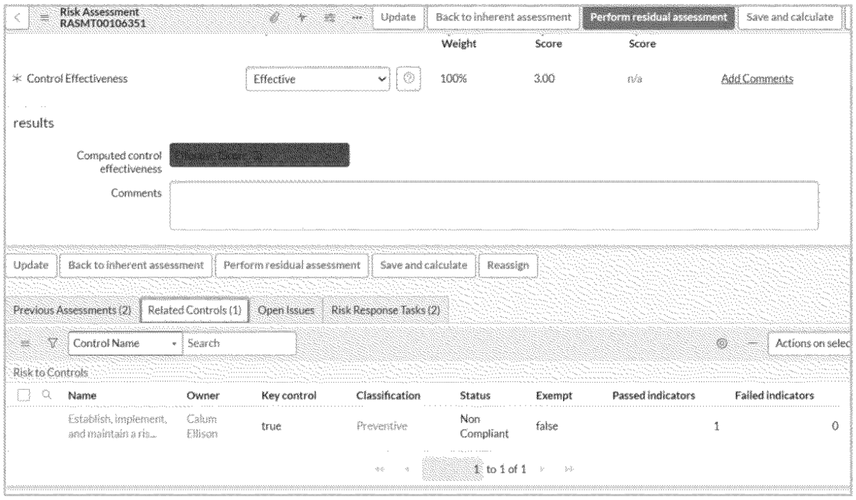


No mitigating controls to assess □

Enter responses for the factors that need manual responses and save the form to view the computed control effectiveness. For automated factors, the responses are automatically calculated.

Factor	Response	Qualitative Weight	Qualitative Score	Quantitative Score	Comments
* Control Effectiveness	Choose here	100%	–	n/a	Add Comments

- If you are 'live' on the Controls Framework assess your controls. Check the Related Controls tab for any controls and consider if the controls would reduce your inherent risk score. You may need to uncheck the no mitigating controls to assess before you can select the Control Effectiveness from the drop-down menu. Control assessment guidance can be viewed by clicking guidance next to Control Effectiveness (refer to paragraph 1.7 for guidance details). If there is any change, add your rationale in the comments box. Select either 'Ineffective', 'Partially effective', or 'Effective' from the drop-down list on the Response field of the Control Assessment tab.
- If there are no controls linked to your risk under the Related Controls tab and they are managed offline for example via excel/SharePoint etc, add a comment in the comment box saying that controls are managed offline and possibly include control numbers (if you have them) or processes you are using. Once you have added your comments, you will need to complete the control effectiveness by clicking the scroll down menu.
- What if you don't have any controls implemented to mitigate the risk? Tick "no mitigating controls to assess'.



Risk Assessment
RASMT00106351

		Weight	Score	Score	
✳ Control Effectiveness	Effective	100%	3.00	n/a	Add Comments

results

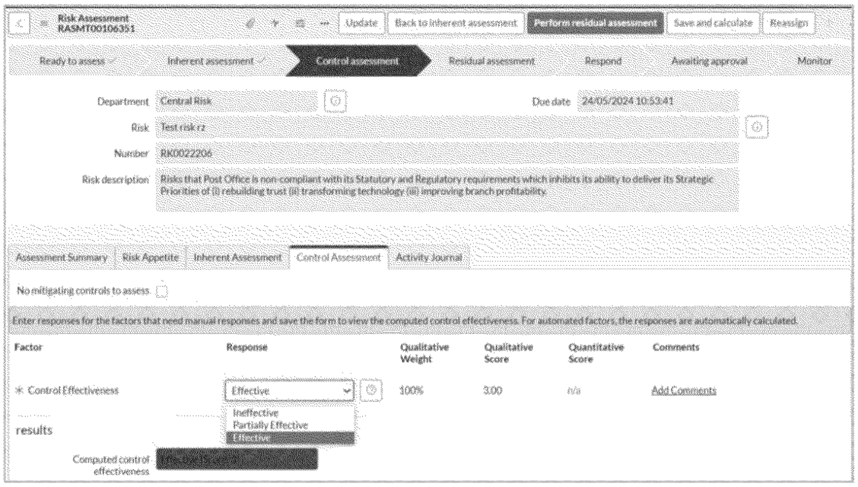
Computed control effectiveness: [illegible]

Comments:

Risk to Controls

Name	Owner	Key control	Classification	Status	Exempt	Passed indicators	Failed indicators
Establish, implement, and maintain a ris...	Calum Ellison	true	Preventive	Non Compliant	false	1	0

1 to 1 of 1



Risk Assessment
RASMT00106351

Department: Central Risk

Due date: 24/05/2024 10:53:41

Risk: Test risk rz

Number: RK0022206

Risk description: Risks that Post Office is non-compliant with its Statutory and Regulatory requirements which inhibits its ability to deliver its Strategic Priorities of (i) rebuilding trust (ii) transforming technology (iii) improving branch profitability.

No mitigating controls to assess ☐

Enter responses for the factors that need manual responses and save the form to view the computed control effectiveness. For automated factors, the responses are automatically calculated.

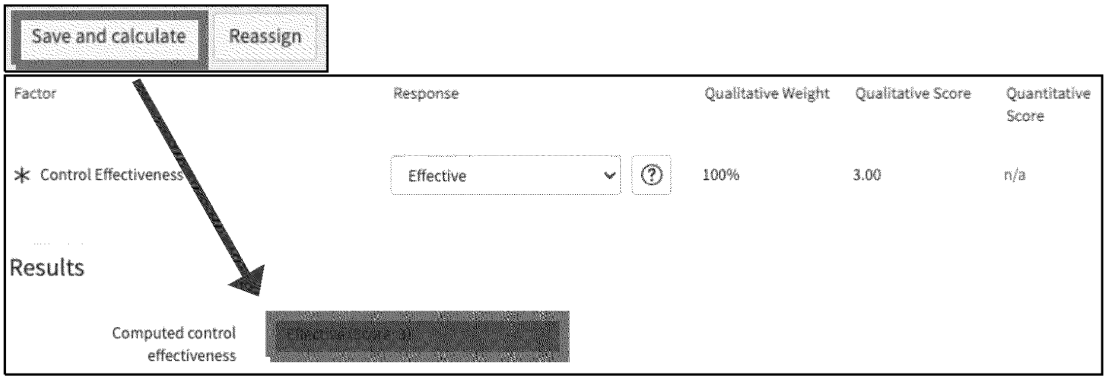
Factor	Response	Qualitative Weight	Qualitative Score	Quantitative Score	Comments
✳ Control Effectiveness	Effective	100%	3.00	n/a	Add Comments

results

Computed control effectiveness: [illegible]

- If there is any change add your rationale in the comments box.

- Once completed, click 'Save and calculate' at the top right hand of the page to calculate Control Effectiveness score.

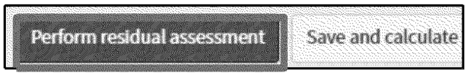


Factor	Response	Qualitative Weight	Qualitative Score	Quantitative Score
✱ Control Effectiveness	Effective	100%	3.00	n/a

Results

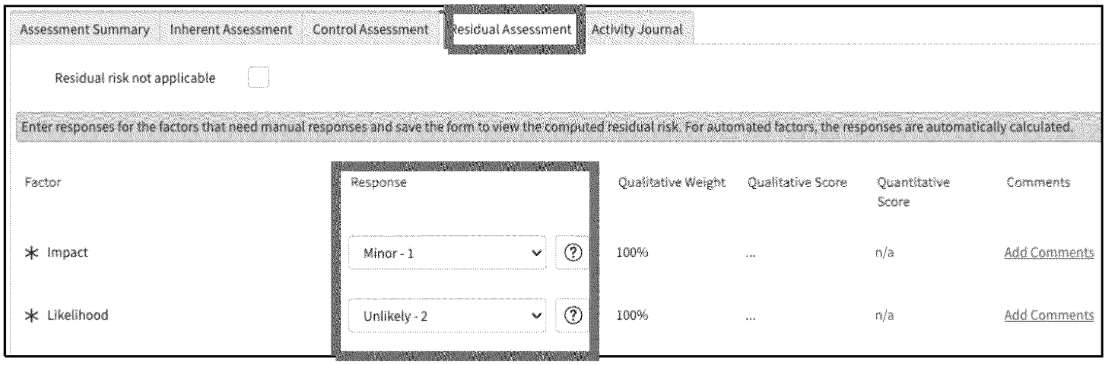
Computed control effectiveness: Effective (Score: 3)

- Click 'Perform residual assessment'.



2.6.6 Residual Assessment

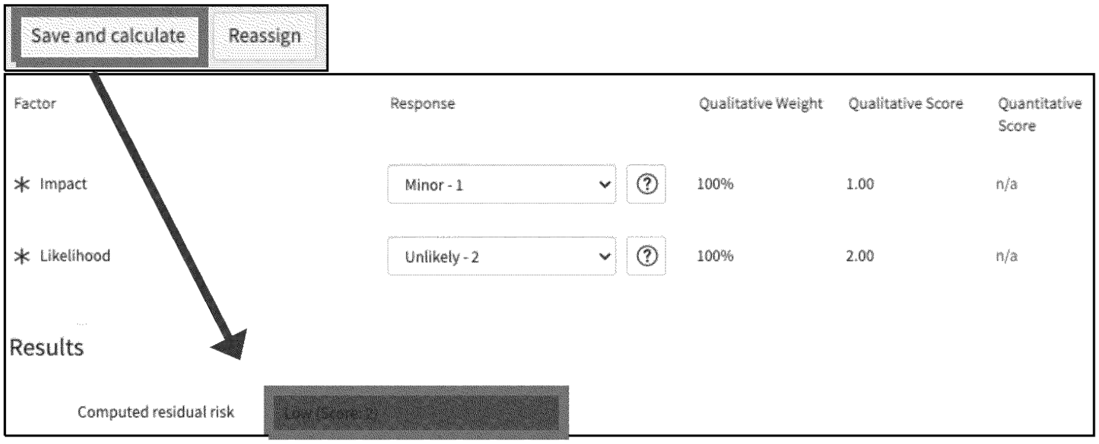
- The 3rd stage of the risk assessment process is the 'Residual Assessment'.
- Check to ensure that the residual risk not applicable box is not ticked to allow for the risk scores to be completed.
- Before assessing your residual score, check the risk appetite and tolerance under the risk appetite tab. All risks should be managed within the agreed risk appetite.
- The residual risk is the latest level of risk considering the effectivenessof the controls currently in place. To complete the residual risk, navigate to the Residual Assessment tab and use the drop-down Response fields for Likelihood and Impact to score the risk, on a 1-5 scale. The residual score can remain the same as previous assessment if the likelihood / impact has not changed, be increased or decreased if the likelihood / impact has changed. Add comments in the comment box with bullet points to provide the reason for the residual score being unchanged or changed after previous assessment. To help you decide you can refer to the Harm Table, which can be viewed by clicking Open from the Guidance next to Impact/Likelihood(refer to paragraph 1.6 for details).
- Click 'Save and calculate' at the top right hand of the page.



Residual risk not applicable □

Enter responses for the factors that need manual responses and save the form to view the computed residual risk. For automated factors, the responses are automatically calculated.

Factor	Response	Qualitative Weight	Qualitative Score	Quantitative Score	Comments
✱ Impact	Minor - 1	100%	...	n/a	Add Comments
✱ Likelihood	Unlikely - 2	100%	...	n/a	Add Comments

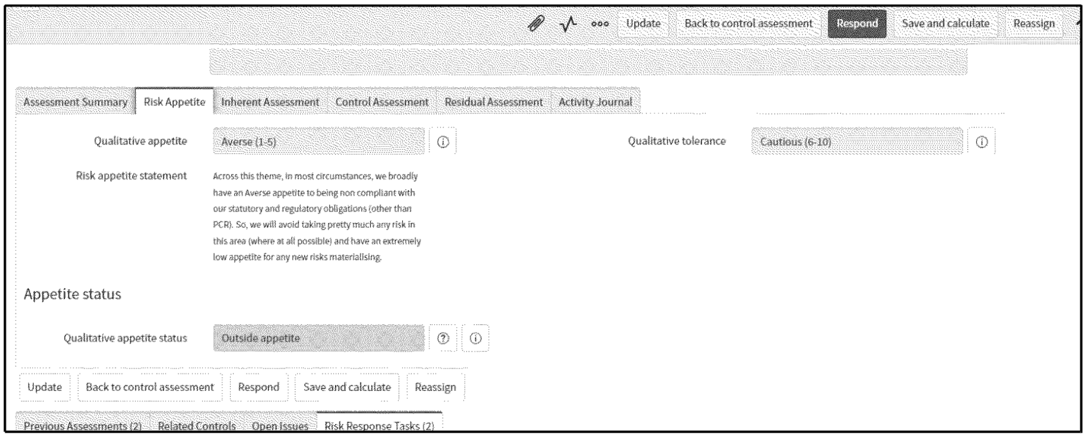


Factor	Response	Qualitative Weight	Qualitative Score	Quantitative Score
✱ Impact	Minor - 1	100%	1.00	n/a
✱ Likelihood	Unlikely - 2	100%	2.00	n/a

Results

Computed residual risk: Low (Score: 2)

- The risk appetite status is populated under the Risk appetite tab to show if the risk is within appetite (green), outside appetite (orange) or outside tolerance (red).



Qualitative appetite: Averse (1-5)

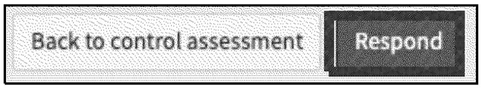
Qualitative tolerance: Cautious (6-10)

Risk appetite statement: Across this theme, in most circumstances, we broadly have an Averse appetite to being non compliant with our statutory and regulatory obligations (other than PCR). So, we will avoid taking pretty much any risk in this area (where at all possible) and have an extremely low appetite for any new risks materialising.

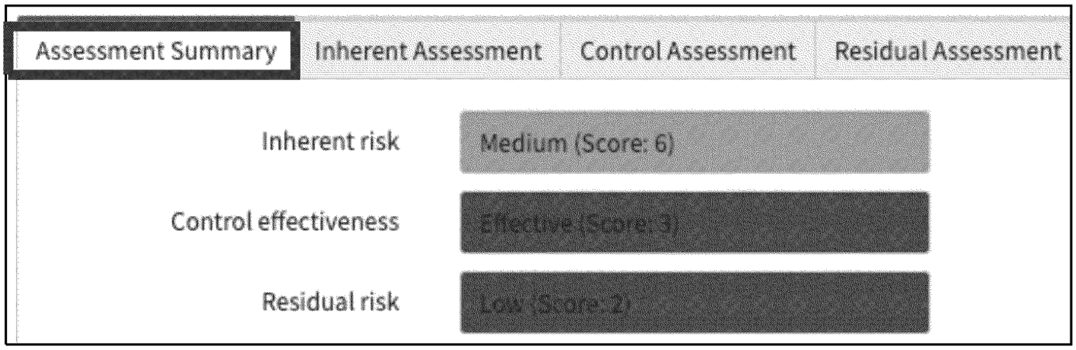
Appetite status

Qualitative appetite status: Outside appetite

- Complete the risk assessment by clicking 'Respond'.



- The risk assessment result is automatically reflected in the risk record and can be located on the 'Assessment Summary' tab:



Inherent risk: Medium (Score: 6)

Control effectiveness: Effective (Score: 3)

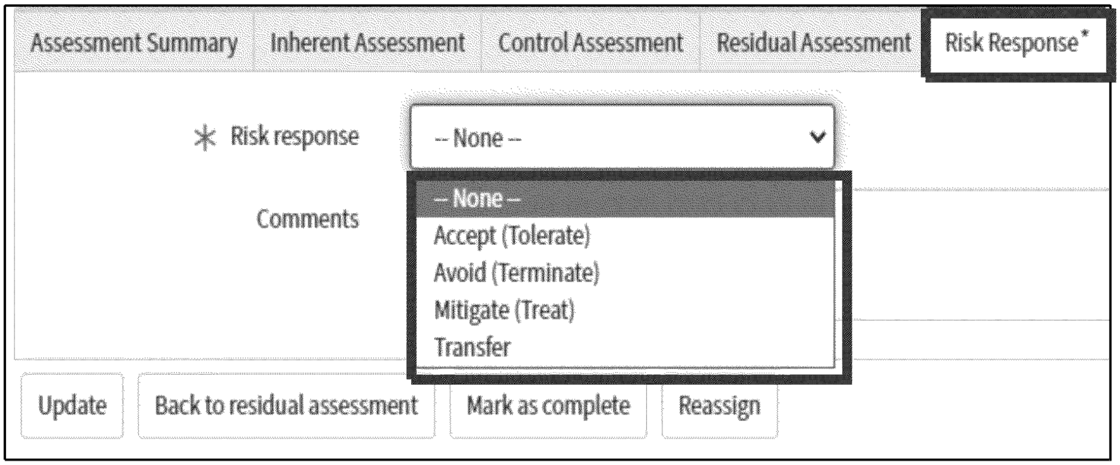
Residual risk: Low (Score: 2)

2.6.7 Risk Response

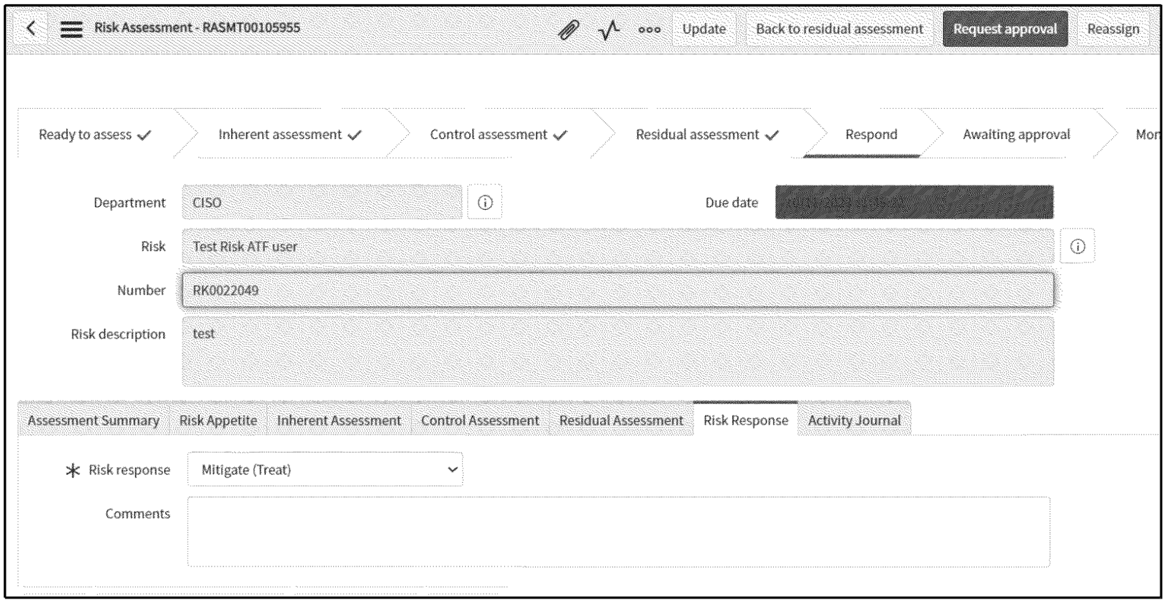
- Risks automatically move to the respond state once assessment is complete, and the 'Risk Response' tab becomes active. Select this tab and a Risk Response to the risk assessment – Mitigate (Treat), Accept (Tolerate), Avoid (Terminate) or Transfer.
- Check the risk appetite status under the Risk appetite tab. All risks outside of appetite and/or tolerance must have a mitigation plan in place to ensure the risk is brought within these levels and may be presented to the relevant governance forums for escalation/agreement of the risk position. If your risk is outside appetite or tolerance, select Mitigate or Transfer or Avoid.

Risk appetite status	Risk Response
Within appetite	Accept or Mitigate or Transfer or Avoid
Outside appetite	Mitigate or Transfer or Avoid
Outside tolerance	Mitigate or Transfer or Avoid

- For all the above responses, a risk response task is created for you to action (refer toparagraph 2.7 on how to complete these tasks and 1.8 for risk response type).

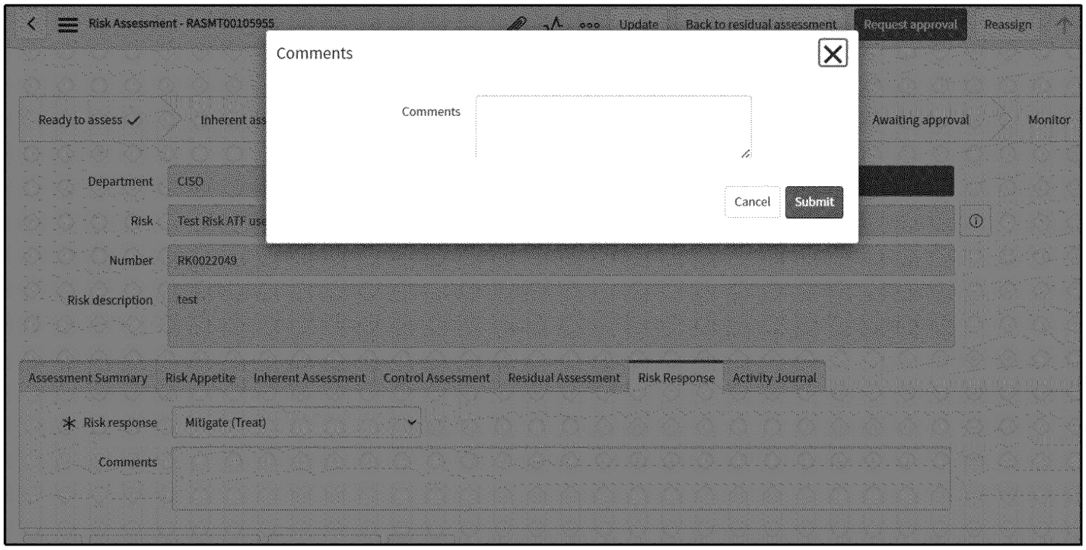


- Once done, click 'Request approval' button



Department	CISO
Due date	[redacted]
Risk	Test Risk ATF user
Number	RK0022049
Risk description	test
* Risk response	Mitigate (Treat)
Comments	

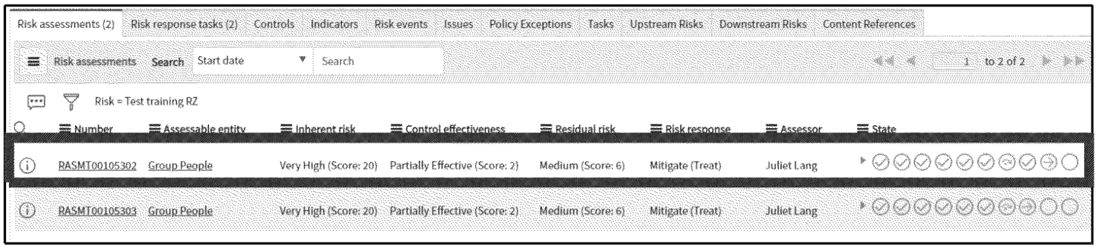
- Click 'Submit'. The risk assessment moves to a 'Monitor' state and the previous risk assessment moves to 'Closed' state. A response record is created and will be visible on your Risk Response tab.



Comments

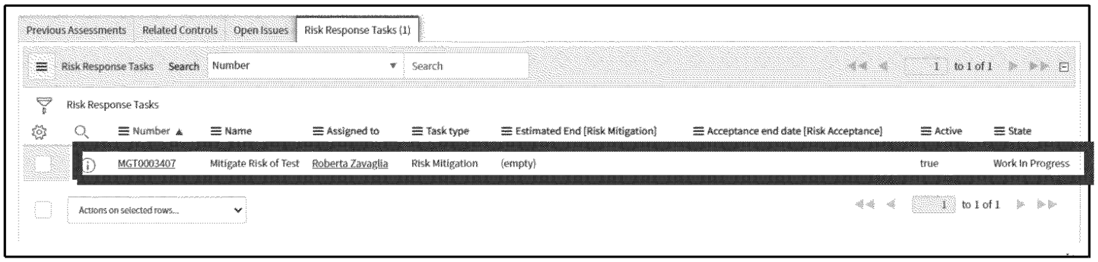
Comments

Cancel Submit



Risk = Test training RZ

Number	Assessable entity	Inherent risk	Control effectiveness	Residual risk	Risk response	Assessor	State
RASMT00105302	Group People	Very High (Score: 20)	Partially Effective (Score: 2)	Medium (Score: 6)	Mitigate (Treat)	Juliet Lang	
RASMT00105303	Group People	Very High (Score: 20)	Partially Effective (Score: 2)	Medium (Score: 6)	Mitigate (Treat)	Juliet Lang	



Number ▲	Name	Assigned to	Task type	Estimated End [Risk Mitigation]	Acceptance end date [Risk Acceptance]	Active	State
MGT0003407	Mitigate Risk of Test	Roberta Zavaglia	Risk Mitigation	(empty)		true	Work In Progress

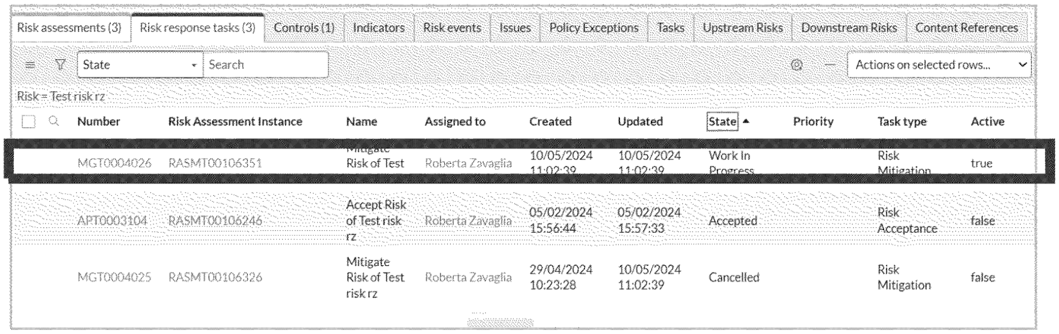
- Once you have completed all risk assessments the ‘My risks assessments ready to assess’ in the Risk User dashboard will now be empty.
- If you have not fully completed an assessment to the end state (i.e. ‘Request Approval’ and ‘Submit’), the assessment will be listed in the middle section of your Risk User dashboard - ‘My Risk Assessments (in Progress)’ list.
- Complete your risk assessments in progress and go back to your Risk User dashboard to check that the section ‘My Risks Assessments (in Progress)’ is now empty.

2.7 COMPLETE A RISK RESPONSE TASK

- Depending on the response selected on the Risk Assessment the system will automatically create and assign to the Risk Assessor one of the following:

2.7.1 Risk Mitigation Task

- Scroll down and click Risk Response Task tab, select the new riskmitigation record created (identified by Active is true or the latest number or a Work in progress state for mitigation task).You can also locate your new risk acceptance task in your Risk User Dashboard - My Open Risk Mitigation Task.

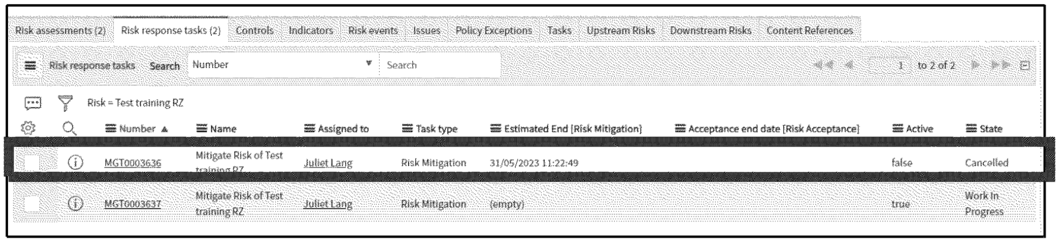


Risk = Test risk rz

Number	Risk Assessment Instance	Name	Assigned to	Created	Updated	State ▲	Priority	Task type	Active
MGT0004026	RASMT00106351	Mitigate Risk of Test	Roberta Zavaglia	10/05/2024 11:02:39	10/05/2024 11:02:39	Work In Progress		Risk Mitigation	true
APT0003104	RASMT00106246	Accept Risk of Test risk rz	Roberta Zavaglia	05/02/2024 15:56:44	05/02/2024 15:57:33	Accepted		Risk Acceptance	false
MGT0004025	RASMT00106326	Mitigate Risk of Test risk rz	Roberta Zavaglia	29/04/2024 10:23:28	10/05/2024 11:02:39	Cancelled		Risk Mitigation	false

- If there is already a mitigation task for your risk, the system automatically cancels your previous open risk response task (i.e. ‘Work in progress’, ‘Awating Approval’ or ‘Review’ state). Risk mitigations in “Closed Complete” state will not be cancelled and remain in closed state.
- You can see your cancelled mitigation task (if applicable) under the “Risk Response Tasks” of your Risk Assessement record.

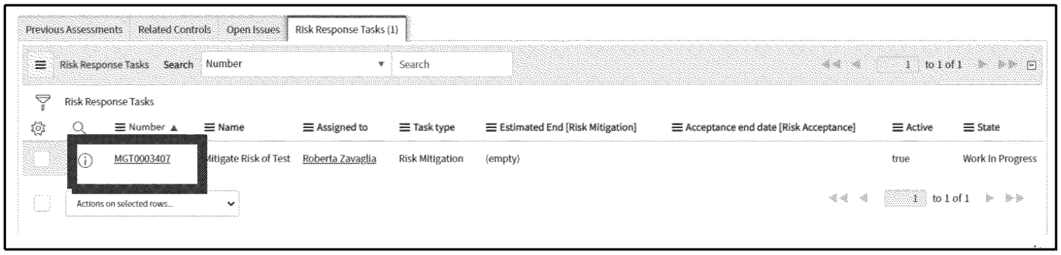
POL00447891



Risk = Test training RZ

Number ▲	Name	Assigned to	Task type	Estimated End [Risk Mitigation]	Acceptance end date [Risk Acceptance]	Active	State
MGT0003636	Mitigate Risk of Test training RZ	Juliet Lang	Risk Mitigation	31/05/2023 11:22:49		false	Cancelled
MGT0003637	Mitigate Risk of Test training RZ	Juliet Lang	Risk Mitigation	(empty)		true	Work In Progress

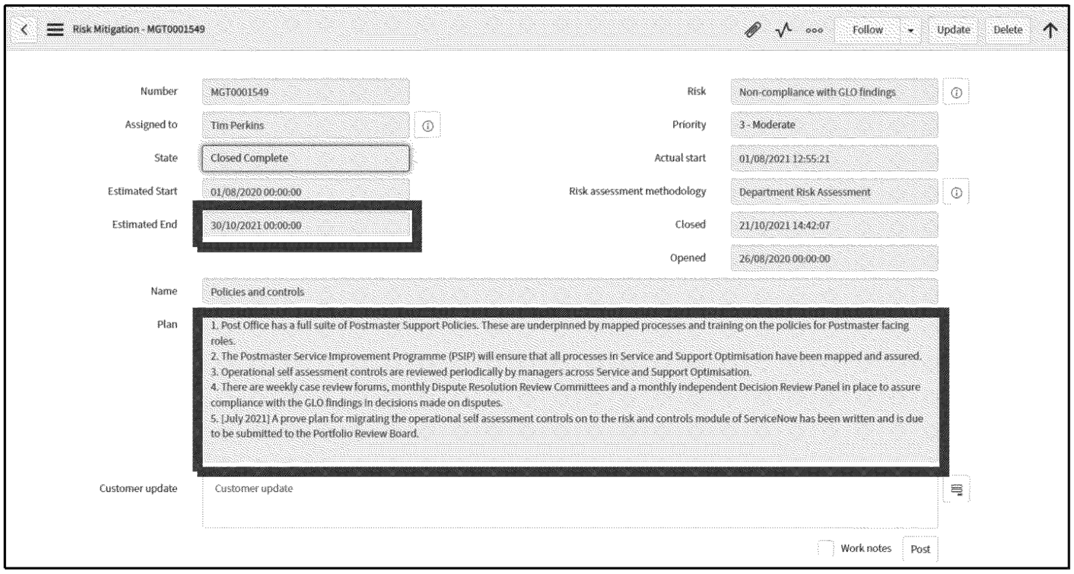
- Click the empty MGT number (not the words).



Risk Response Tasks

Number ▲	Name	Assigned to	Task type	Estimated End [Risk Mitigation]	Acceptance end date [Risk Acceptance]	Active	State
MGT0003407	Mitigate Risk of Test	Roberta Zavaglia	Risk Mitigation	(empty)		true	Work In Progress

- Complete the 'Estimated start date', 'end date' (what is the next key milestone of the remediation or the date you expect the mitigation plan to be completed by).
- Now complete the "Plan". You will have to copy and paste your Plan into the new one ifyour cancelled mitigation was still open (i.e. 'Work in progress', 'Awaiting Approval', 'Review') or complete the new mitigation task with new details if the previous onewas 'Closed Complete'. List bullet points of key actions that will be in place or key projects that will remediate this risk.This is information that will be used to produce risk reports to your GE member and to the Risk and Compliance Committee, so be as clear as possible. This is a good example:



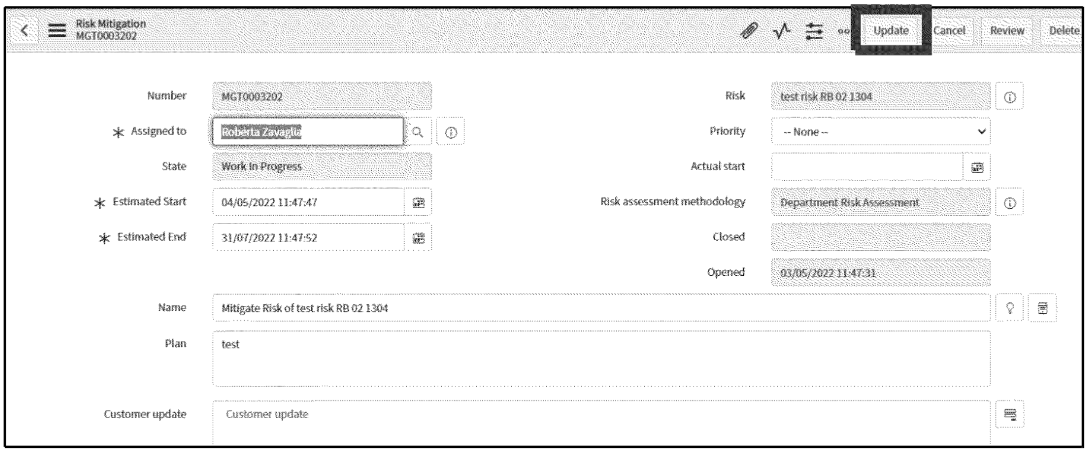
Number	MGT0001549	Risk	Non-compliance with GLO findings
Assigned to	Tim Perkins	Priority	3 - Moderate
State	Closed Complete	Actual start	01/08/2021 12:55:21
Estimated Start	01/08/2020 00:00:00	Risk assessment methodology	Department Risk Assessment
Estimated End	30/10/2021 00:00:00	Closed	21/10/2021 14:42:07
		Opened	26/08/2020 00:00:00

Name: Policies and controls

Plan:
1. Post Office has a full suite of Postmaster Support Policies. These are underpinned by mapped processes and training on the policies for Postmaster facing roles.
2. The Postmaster Service Improvement Programme (PSIP) will ensure that all processes in Service and Support Optimisation have been mapped and assured.
3. Operational self assessment controls are reviewed periodically by managers across Service and Support Optimisation.
4. There are weekly case review forums, monthly Dispute Resolution Review Committees and a monthly independent Decision Review Panel in place to assure compliance with the GLO findings in decisions made on disputes.
5. [July 2021] A prove plan for migrating the operational self assessment controls on to the risk and controls module of ServiceNow has been written and is due to be submitted to the Portfolio Review Board.

Customer update: Customer update

- Once updated click "Update", your risk response will remain in Work in progress state.You have now reviewed and update your new plan.



Number	MGT0003202	Risk	test risk RB 02 1304
* Assigned to	Roberta Zavaglia	Priority	-- None --
State	Work In Progress	Actual start	
* Estimated Start	04/05/2022 11:47:47	Risk assessment methodology	Department Risk Assessment
* Estimated End	31/07/2022 11:47:52	Closed	
		Opened	03/05/2022 11:47:31
Name	Mitigate Risk of test risk RB 02 1304		
Plan	test		
Customer update	Customer update		

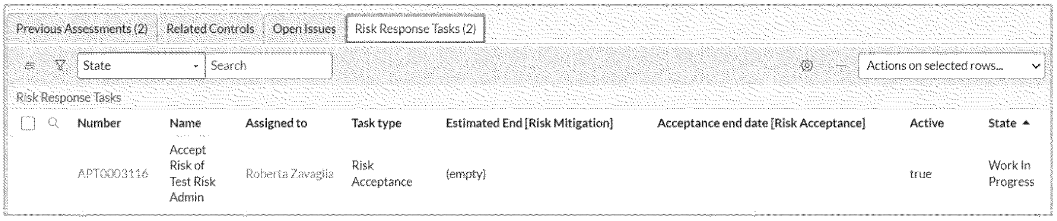
- If you mitigation is in 'Work in progresss', You can update your risk mitigation plan at any time. You do not need to wait for a risk assessment to be released.
- Ask your RBP if you need any help.

Risk mitigation closure

- You can close a mitigation plan, if the risk is either in an (i) Accept state or (ii) no longer exists. If it is point (i) Contact your RBP who will release an assessment for you to complete which will enable you to rescore the risk and enter Accept in the respond section (see acceptance response task section below). If it is point (ii), refer to paragraph 2.8 for how to retire a risk.
- Once your mitigation is 'Closed Complete', the risk record will move to 'Monitor' state and it will be in read-only, so you will not be able to edit any risk details (including risk name, description, statement etc.). Your risk record will be editable again as soon as a new risk assessment is released. Your risk mitigation task will be also not editable. **Please DO NOT close your mitigation if you wish to edit your risk record or your mitigation record until your next risk assessment release.**

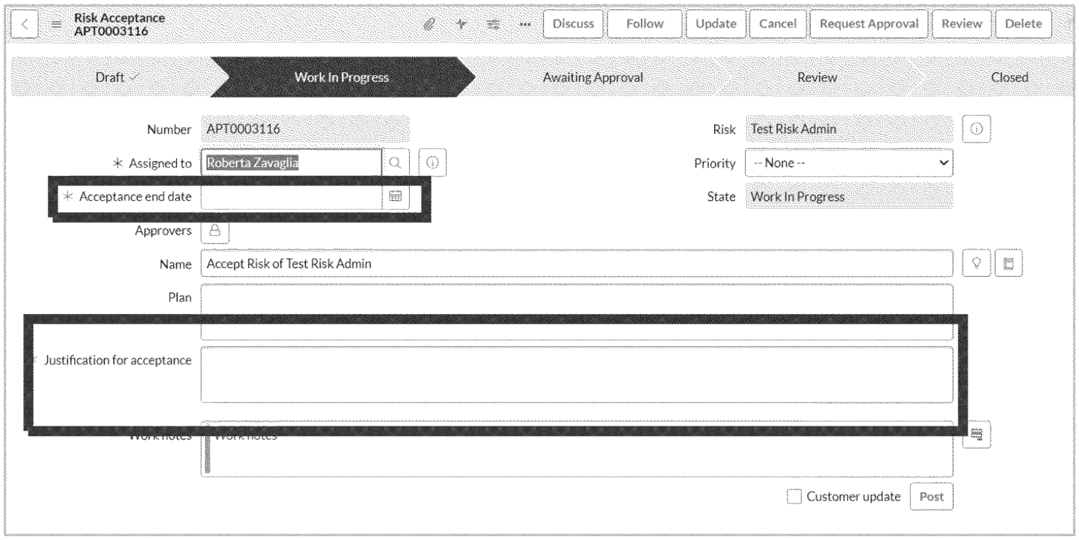
2.7.2 Risk Acceptance Task

- Scroll down and click Risk Response Task tab, select the new risk acceptance record created (identified by Active is true or the latest number or a Work in progress state for mitigation task). You can also locate your new risk acceptance task in your Risk User Dashboard - My Open Risk Acceptance Task.
- Click on the APT number (not the words). If the risk has been accepted before there will be more than one risk acceptance tasks showing.



Number	Name	Assigned to	Task type	Estimated End [Risk Mitigation]	Acceptance end date [Risk Acceptance]	Active	State ▲
APT0003116	Accept Risk of Test Risk Admin	Roberta Zavaglia	Risk Acceptance	(empty)		true	Work In Progress

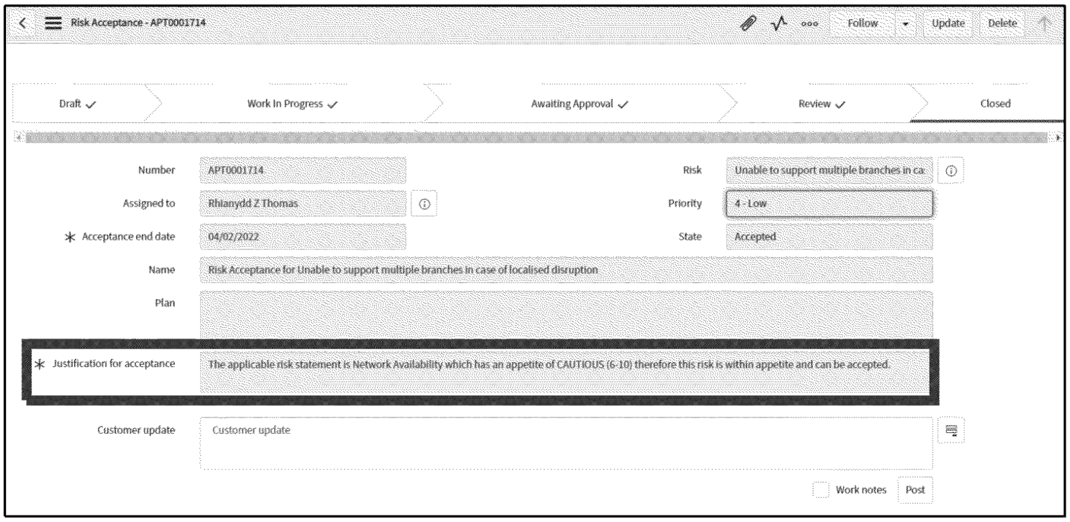
- The system will automatically cancel your previous open risk response task (i.e. 'Work in progress', 'Awating Approval' or 'Review' state). Risk acceptances in 'Accepted'/'Closed' state will not be cancelled.



Risk Acceptance
APT0003116

Number: APT0003116
* Assigned to: Roberta Zavaglia
* Acceptance end date:
Approvers:
Name: Accept Risk of Test Risk Admin
Plan:
Justification for acceptance:
Work notes: Work notes
Risk: Test Risk Admin
Priority: -- None --
State: Work In Progress

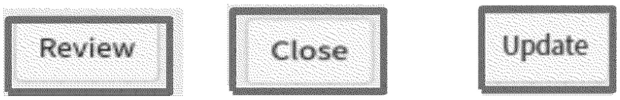
- Enter the 'Acceptance end date'. This is how long you are prepared to accept the risk for without reviewing it, and we would recommend that this is no more than 12 months. When the 'Acceptance end date' passes the system will automatically release a Risk Assessment to the Risk Owner.
- Complete the 'Plan' with the event that is driving the acceptance end date(e.g. Our Strategic plan will be finalized by the xx/xx/xx which may impact on this risk). The Plan must be relevant to the risk
- Complete the 'Justification for acceptance' section. This is a short confirmation as to why you have agreed to accept this risk for the agreed period of time. This would usually be because the risk is within the business's risk appetite. This is an example of justfication for acceptance:



Risk Acceptance - APT0001714

Number: APT0001714
Assigned to: Rhianydd Z Thomas
* Acceptance end date: 04/02/2022
Name: Risk Acceptance for Unable to support multiple branches in case of localised disruption
Plan:
* Justification for acceptance: The applicable risk statement is Network Availability which has an appetite of CAUTIOUS (6-10) therefore this risk is within appetite and can be accepted.
Customer update: Customer update
Risk: Unable to support multiple branches in ca
Priority: 4 - Low
State: Accepted

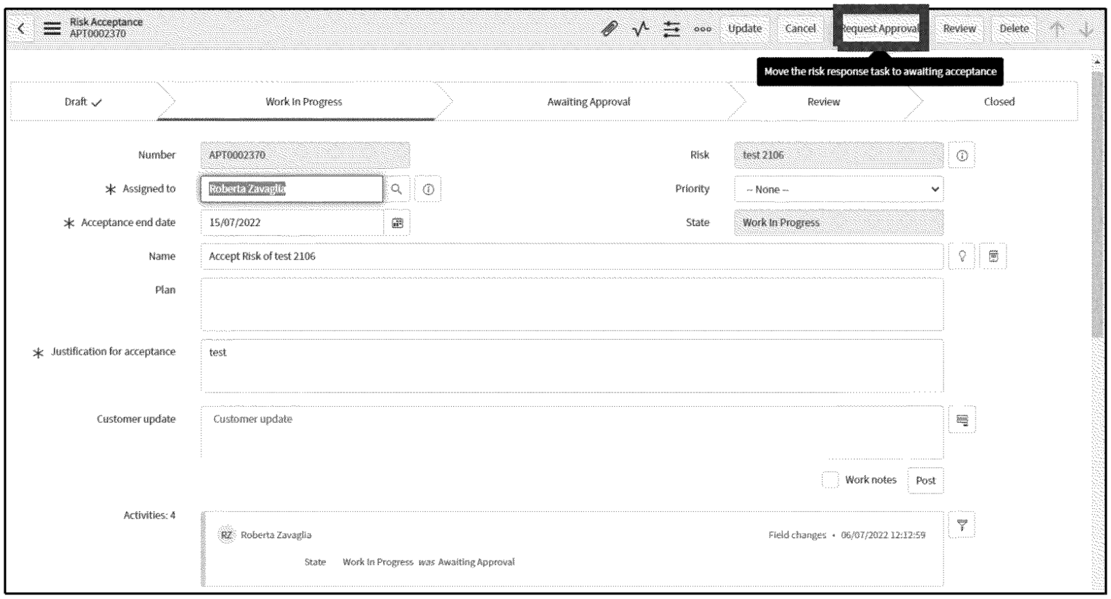
- Click the 'Review' button and then 'Close' button. Do not click any other buttons as this will prevent the task being completed to the Accepted state. This is very important as if this is notcompleted correctly, a risk assessment will not be released in the future.



- You have now fully completed the Acceptance task.
- Once your acceptance is ‘Accepted’, the risk record will move to ‘Monitor’ state and it will be in read-only, so you will not be able to edit any risk details (including risk name, description, statement etc.).Your risk record will be editable again as soon as a new risk assessment is released. Your risk acceptance task will be also not editable.
- Go back to your Risk User dashboard and the section ‘My open Acceptance Tasks ’ should now be empty.
- If your assessment of the risk (or its controls, or your risk appetite) changes and you no longer want to accept the risk before the acceptance end date is reached contact your Risk Business Partner who can release the risk for assessment.

ACCEPTANCE TASK DELEGATED

- When the risk assessment is delegated to someone other than the risk owner, the delegated person should request approval by clicking the ‘Request Approval’ button on the top right The risk response acceptance task is moved to the ‘Awaiting Approval’ state.



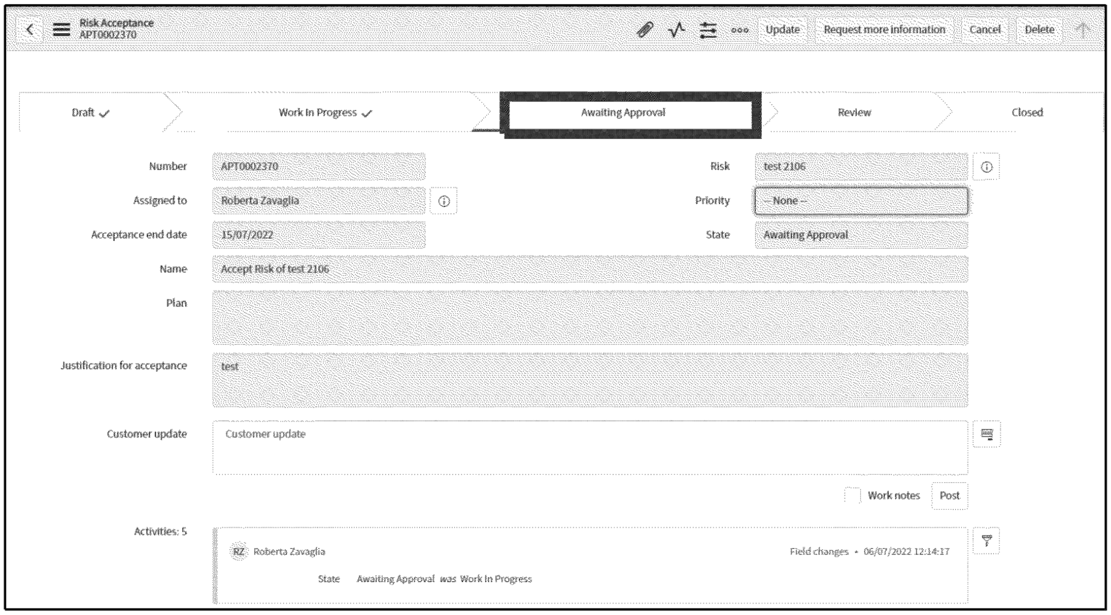
Number	APT0002370	Risk	test 2106
* Assigned to	Roberta Zavaglia	Priority	-- None --
* Acceptance end date	15/07/2022	State	Work In Progress
Name	Accept Risk of test 2106		
Plan			
* Justification for acceptance	test		
Customer update	Customer update		

Activities: 4

RZ Roberta Zavaglia — Field changes • 06/07/2022 12:12:59

State Work In Progress *was* Awaiting Approval

POL00447891



Risk Acceptance
APT0002370

Number	APT0002370	Risk	test 2106
Assigned to	Roberta Zavaglia	Priority	-- None --
Acceptance end date	15/07/2022	State	Awaiting Approval

Name: Accept Risk of test 2106

Plan:

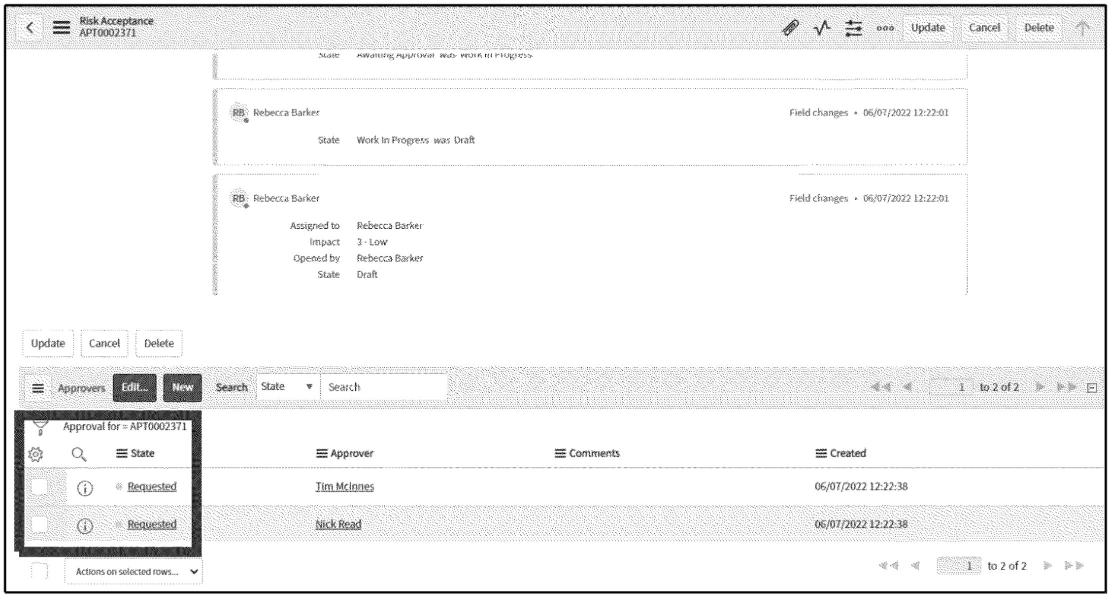
Justification for acceptance: test

Customer update: Customer update

Activities: 5

RZ Roberta Zavaglia — Field changes • 06/07/2022 12:14:17
State Awaiting Approval *was* Work In Progress

- Risk owners should not request approval of their tasks.
- Delegates can view approvers on the risk acceptance task record under ‘Approvers’.



Risk Acceptance
APT0002371

State Awaiting Approval *was* Work In Progress

RB Rebecca Barker — Field changes • 06/07/2022 12:22:01
State Work In Progress *was* Draft

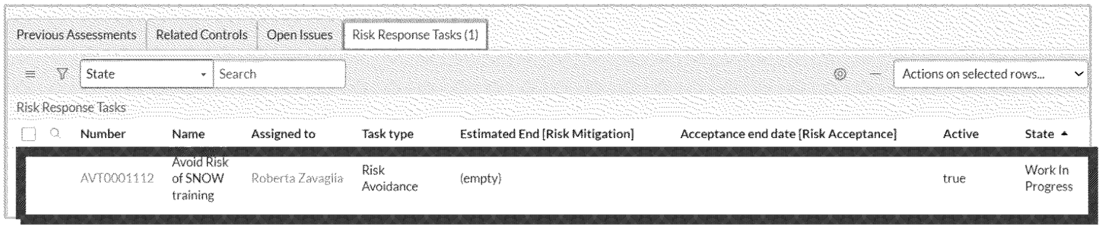
RB Rebecca Barker — Field changes • 06/07/2022 12:22:01
Assigned to Rebecca Barker
Impact 3 - Low
Opened by Rebecca Barker
State Draft

Approval for = APT0002371

State	Approver	Comments	Created
Requested	Tim McInnes		06/07/2022 12:22:38
Requested	Nick Read		06/07/2022 12:22:38

2.7.3 Risk Avoidance Task

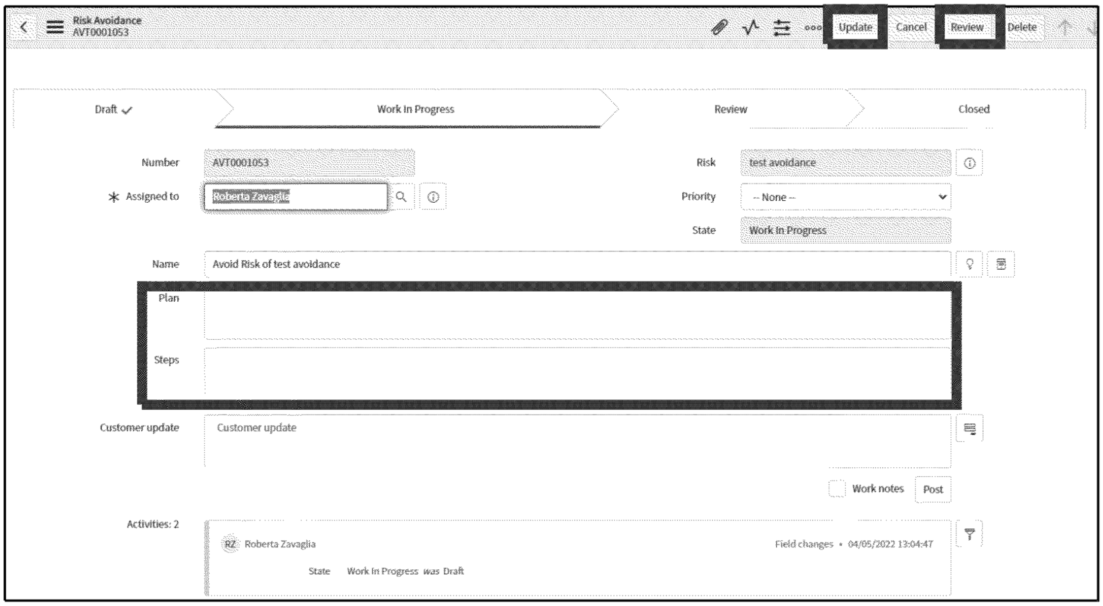
- Scroll down and click Risk Response Task tab if you are still perfoming your risk assessment or log into ServiceNow and load your Risk User dashboard – **My Open Risk Avoidance Tasks**.
- Select the new risk avoidance record created (identified by Active is true or the latest number or a Work in progress state for mitigation task)
- Click on the AVT number (not the words).



Risk Response Tasks

Number	Name	Assigned to	Task type	Estimated End [Risk Mitigation]	Acceptance end date [Risk Acceptance]	Active	State
AVT0001112	Avoid Risk of SNOW training	Roberta Zavaglia	Risk Avoidance	(empty)		true	Work In Progress

- The system will automatically cancel your previous open risk response task, as mentioned in paragraph 2.7.1 and 2.7.2.
- Enter Plan and Steps to implement the plan.
- Click 'Update', 'Review' and 'Close' button, when you are satisfied with the plan. Your task will be in Closed state.
- Once your avoidance is 'Closed', the risk record will move to 'Monitor' state andboth risk and response task records will be in read-only, as mentioned in paragraph 2.7.1 and 2.7.2.

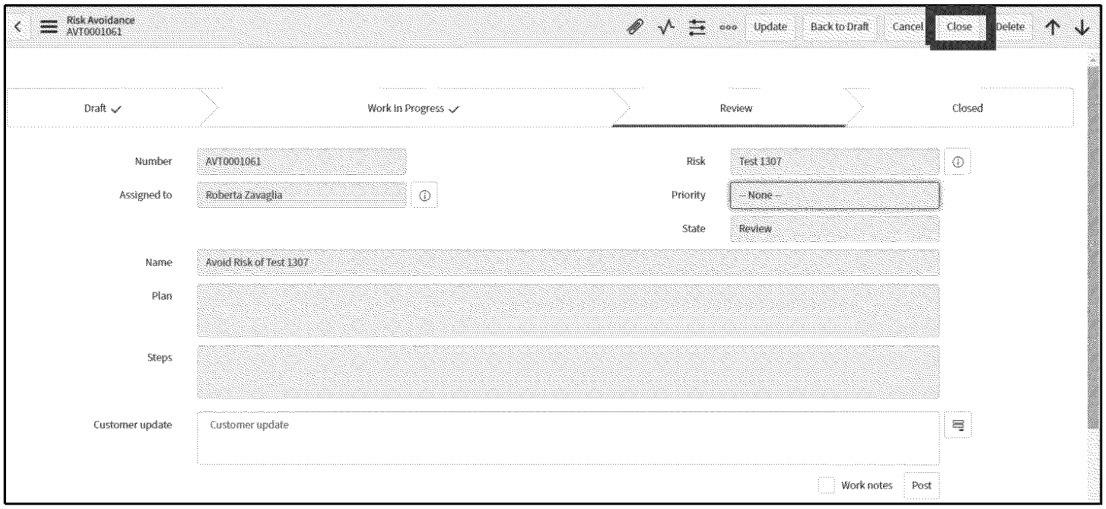


Number	AVT0001053
* Assigned to	Roberta Zavaglia
Risk	test avoidance
Priority	-- None --
State	Work In Progress
Name	Avoid Risk of test avoidance
Plan	
Steps	
Customer update	Customer update

Activities: 2

RZ Roberta Zavaglia Field changes • 04/05/2022 13:04:47

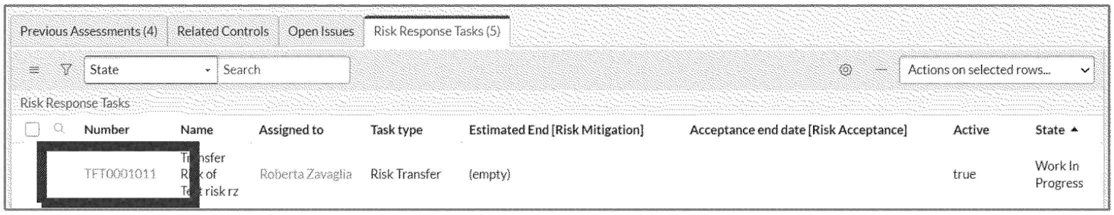
State Work In Progress *was* Draft



Number	AVT0001061	Risk	Test 1307
Assigned to	Roberta Zavaglia	Priority	-- None --
		State	Review
Name	Avoid Risk of Test 1307		
Plan			
Steps			
Customer update	Customer update		

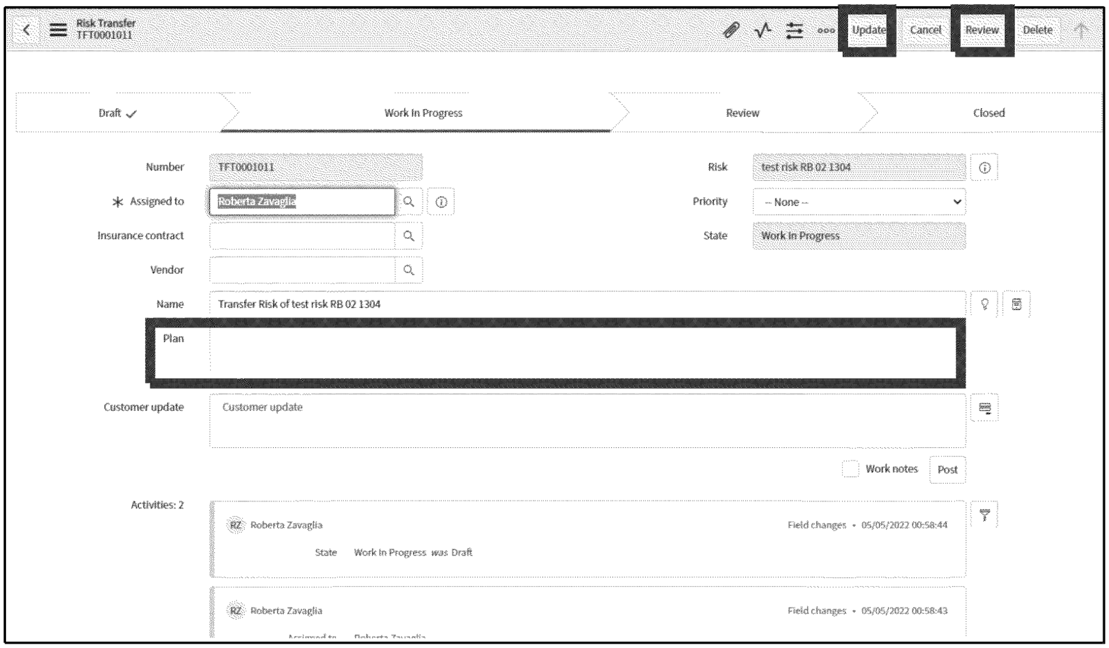
2.7.4 Risk Transfer Task

- Scroll down and click Risk Response Task tab if you are still perfoming your risk assessment or log into ServiceNow and load your Risk User dashboard – **My Open Risk Transfer Tasks**.
- Select the new risk transfer record created (identified by Active is true or the latest number or a Work in progress state for mitigation task)
- Click on the TFT number (not the words).
- The system will automatically cancel your previous open risk response task, as mentioned in paragraph 2.7.1 and 2.7.2.



Number	Name	Assigned to	Task type	Estimated End [Risk Mitigation]	Acceptance end date [Risk Acceptance]	Active	State ▲
TFT0001011	Transfer Risk of Test risk rz	Roberta Zavaglia	Risk Transfer	(empty)		true	Work In Progress

- Enter the ‘Plan’ details.
- Click ‘Update’, ‘Review’ and ‘Close’ button, when you are satisfied with the plan. Your task will be in Closed state.
- Once your transfer is ‘Closed’, the risk record will move to ‘Monitor’ state and both risk and response task records will be in read-only, as mentioned in paragraph 2.7.1 and 2.7.2.



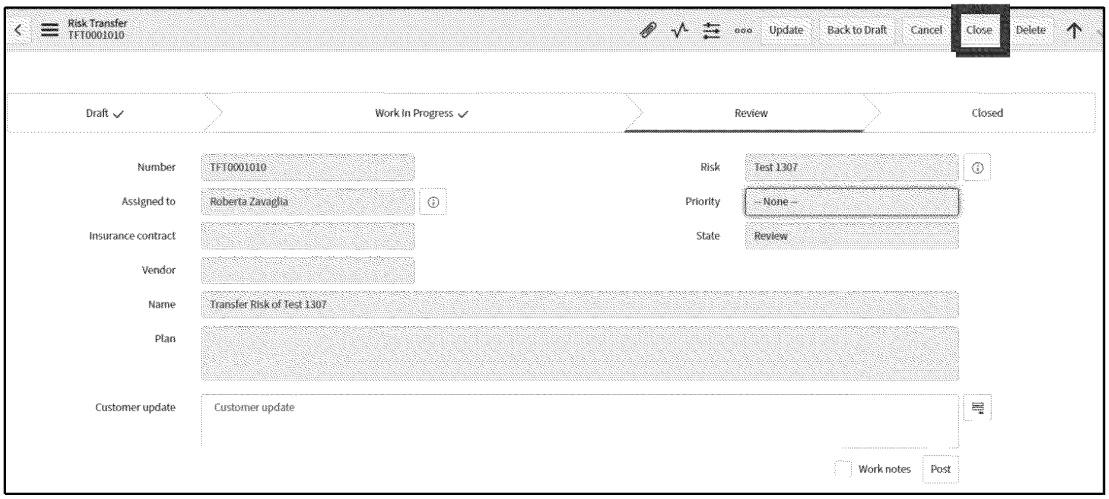
Number: TFT0001011
Risk: test risk RB 02 1304
Assigned to: Roberta Zavaglia
Priority: -- None --
Insurance contract:
State: Work In Progress
Vendor:
Name: Transfer Risk of test risk RB 02 1304
Plan:
Customer update: Customer update

□ Work notes

Activities: 2

RZ Roberta Zavaglia — Field changes • 05/05/2022 00:58:44
State — Work In Progress *was* Draft

RZ Roberta Zavaglia — Field changes • 05/05/2022 00:58:43
Assigned to — Roberta Zavaglia

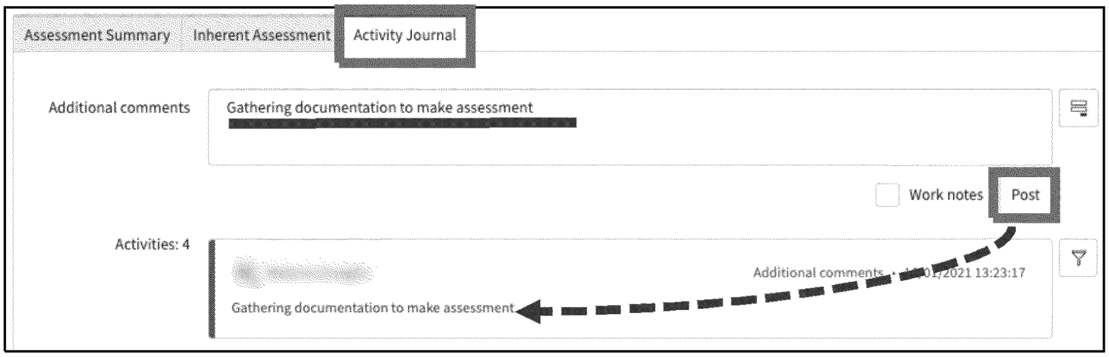


Number: TFT0001010
Risk: Test 1307
Assigned to: Roberta Zavaglia
Priority: -- None --
Insurance contract:
State: Review
Vendor:
Name: Transfer Risk of Test 1307
Plan:
Customer update: Customer update

□ Work notes

2.7.5 Activity Journal

- Your RBP will use the 'Additional comments' box of the Activity Journal tab to communicate with you tagging you in.
- You can add notes/communication in the 'Additional comments' box and interact with your RBP or other risk users using the tagging functionality @ and then entering the name of the person you want to mention.
- You can click 'Post' to move additional comment to Activities stream.

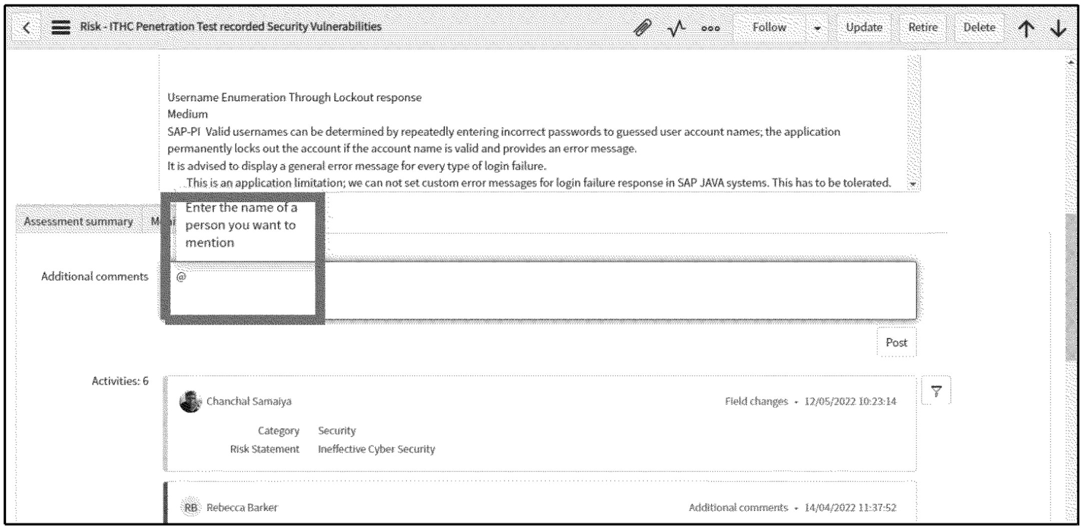


Additional comments: Gathering documentation to make assessment
[redacted]

Activities: 4

[redacted] Additional comments • 1…01/2021 13:23:17

Gathering documentation to make assessment


Risk - ITHC Penetration Test recorded Security Vulnerabilities
Follow
Update
Retire
Delete

Username Enumeration Through Lockout response
Medium
SAP-PI Valid usernames can be determined by repeatedly entering incorrect passwords to guessed user account names; the application permanently locks out the account if the account name is valid and provides an error message.
It is advised to display a general error message for every type of login failure.
This is an application limitation; we can not set custom error messages for login failure response in SAP JAVA systems. This has to be tolerated.

Enter the name of a person you want to mention

Additional comments: @

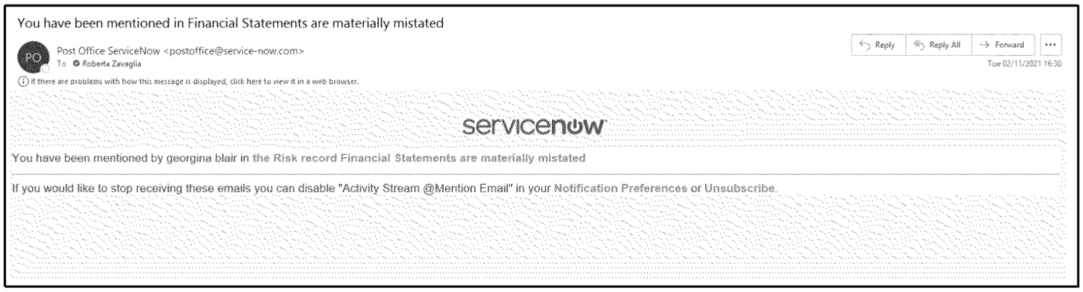
Activities: 6

Chanchal Samaiya Field changes • 12/05/2022 10:23:14

Category	Security
Risk Statement	Ineffective Cyber Security

RB Rebecca Barker Additional comments • 14/04/2022 11:37:52

- You will receive email notifications in your Outlook if you have been tagged in anycommunication.


You have been mentioned in Financial Statements are materially mistated

PO Post Office ServiceNow <postoffice@service-now.com>
To Roberta Zavaglia

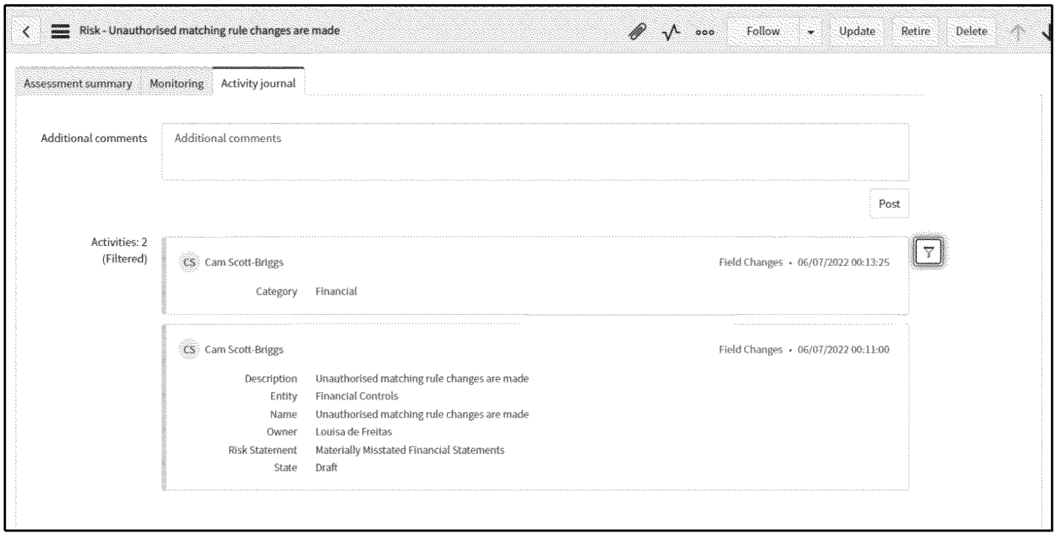
If there are problems with how this message is displayed, click here to view it in a web browser.

You have been mentioned by georgina blair in the Risk record Financial Statements are materially mistated

If you would like to stop receiving these emails you can disable "Activity Stream @Mention Email" in your Notification Preferences or Unsubscribe.

- In the Activity Journal you can also see changes to your risks related to to Category, Description, Entity, Name, Owner, Risk Statement and State.

POL00447891



Additional comments: Additional comments

Activities: 2 (Filtered)

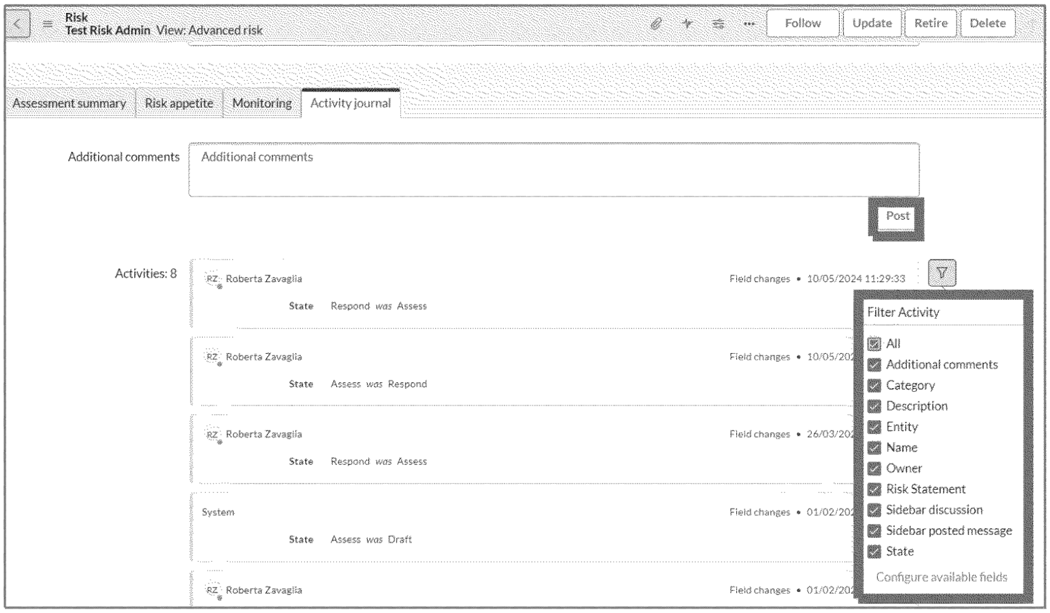
CS Cam Scott-Briggs — Field Changes • 06/07/2022 00:13:25

Category: Financial

CS Cam Scott-Briggs — Field Changes • 06/07/2022 00:11:00

Description: Unauthorised matching rule changes are made
Entity: Financial Controls
Name: Unauthorised matching rule changes are made
Owner: Louisa de Freitas
Risk Statement: Materially Misstated Financial Statements
State: Draft

- You can use the 'Filter Activity' functionality to choose the kind of communication thatyou want to see in your Activity journal (i.e. Additional comments only, risk changes related to Category, Description, Entity, Name, Owner, Risk Statement and State).



Additional comments: Additional comments

Activities: 8

RZ Roberta Zavaglia — Field changes • 10/05/2024 11:29:33
State: Respond *was* Assess

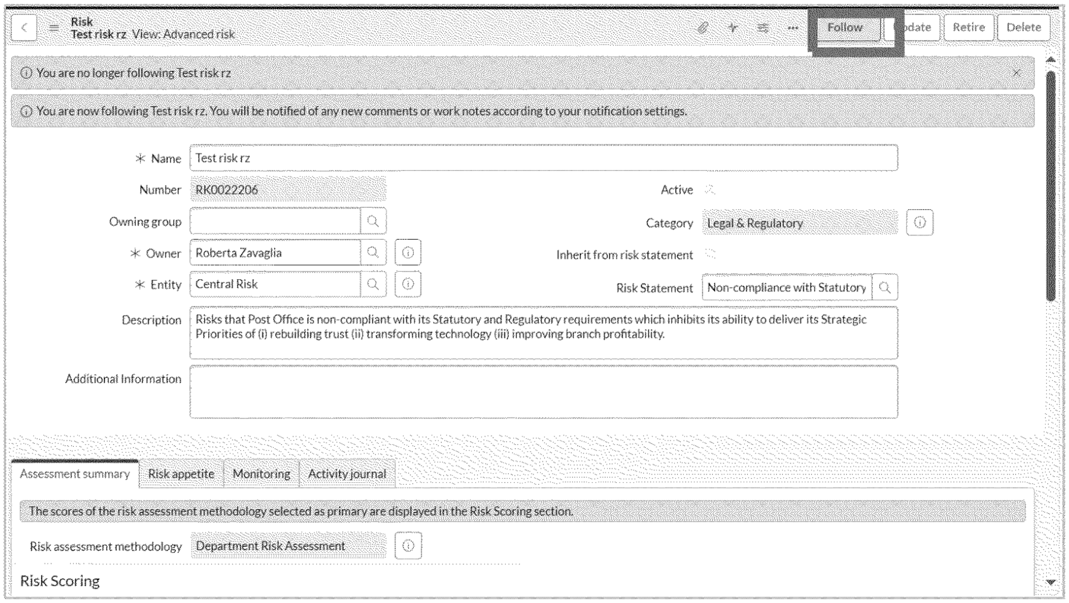
RZ Roberta Zavaglia — Field changes • 10/05/202
State: Assess *was* Respond

RZ Roberta Zavaglia — Field changes • 26/03/202
State: Respond *was* Assess

System — Field changes • 01/02/202
State: Assess *was* Draft

RZ Roberta Zavaglia — Field changes • 01/02/202

- You can use the functionality "Follow" to follow updates on oneparticular risk;



Test risk rz View: Advanced risk

ⓘ You are no longer following Test risk rz

ⓘ You are now following Test risk rz. You will be notified of any new comments or work notes according to your notification settings.

* Name	Test risk rz		
Number	RK0022206	Active	
Owning group		Category	Legal & Regulatory
* Owner	Roberta Zavaglia	Inherit from risk statement	
* Entity	Central Risk	Risk Statement	Non-compliance with Statutory

Description: Risks that Post Office is non-compliant with its Statutory and Regulatory requirements which inhibits its ability to deliver its Strategic Priorities of (i) rebuilding trust (ii) transforming technology (iii) improving branch profitability.

Additional Information:

The scores of the risk assessment methodology selected as primary are displayed in the Risk Scoring section.

Risk assessment methodology: Department Risk Assessment

- You will receive notifications on your Outlook if there are any updates onyour risk or if you have been tagged in any communication.

2.8 RETIRE / CLOSE A RISK

If the risk no longer exists and therefore does not require further assessment or monitoring and you wish to Retire or 'Close' the risk, contact your RBP.