URM

ULTIMA RISK MANAGEMENT

Abriska:
Risk Assessment

User Guide

Ultima Risk Management Limited

Abriska

1.0 Setting up the risk assessment module

1.1 Risk assessment setup

1.1.1 Risk Variables

1.1.1.1 What are Risk Variables?

Abriska allows the risk methodology it uses to be tailored to an organisations specific requirement, by allowing different risk variables to be used to assess threats. For example, impact, likelihood, probability or proximity. URM will initially setup the product to utilise its own risk assessment methodology which can then be tailored to reflect an organisation specific risk appetite or any existing model.

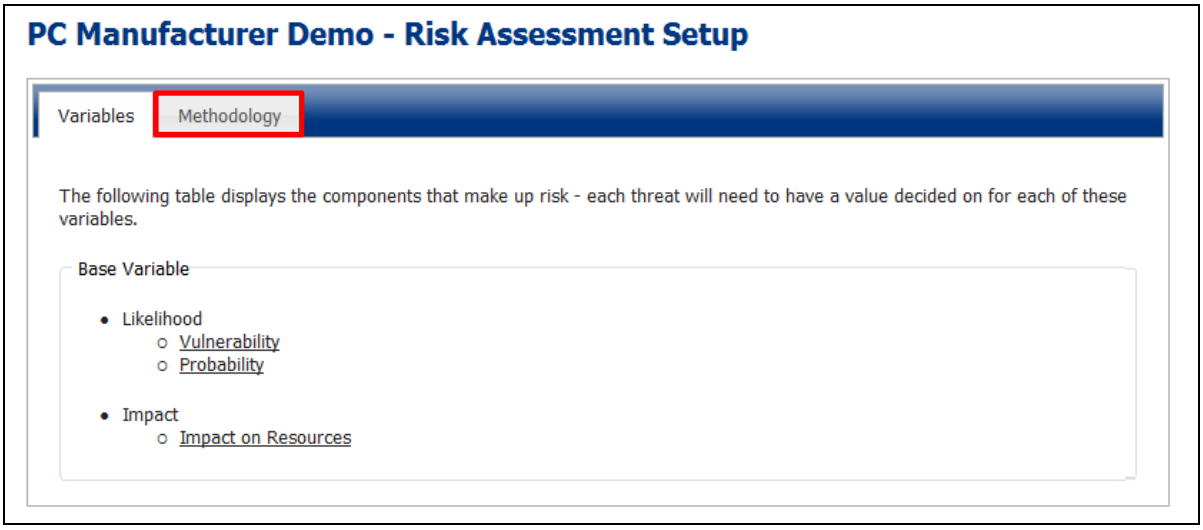


Figure 1 - Risk variables

The explanation of the chosen methodology is available from the methodology tab (highlighted red in Figure 1 - Risk variables).

URM's methodology is as follows:

Likelihood – "*the chance of something happening*". This is made up of two factors:

1. Vulnerability – This is a measure of how much control an organisation has over a potential threat occurring. If an organisation has strong controls in place to mitigate a threat, then this score will be low. However, if there are potential weaknesses or improvements that could be made then this score could be higher.
2. Probability – This is a measure of any external factors that are outside of an organisations control. For example, a pandemic may be certain to happen within the next 2 years. The higher the probability, the more certain an event is to happen.

The default method for calculating a likelihood score is to average the two variables below.

Impact – "*evaluated consequence of a particular outcome*". This is made up from only one factor:

1. Impact on resources – This is the direct impact inflicted on an organisation as a result of the threat occurring. For example, if a flood would result in destruction of assets then this impact would need to be quantified.

Note: URM can assist an organisation define a suitable risk assessment methodology.

1.1.2 Risk Appetite

1.1.2.1 What is the risk appetite?

BS 25999 defines risk appetite as the:

"*total amount of risk that an organisation is prepared to accept, tolerate or be exposed to at any point in time*"

Abriska uses a standard Red-Amber-Green (RAG) matrix to represent an organisations tolerance to any specific risks (shown in Figure 2 - Risk appetite). The risk appetite is viewable by clicking on "RA Setup" from the main organisation screen, then selecting "Setup Risk Appetite".

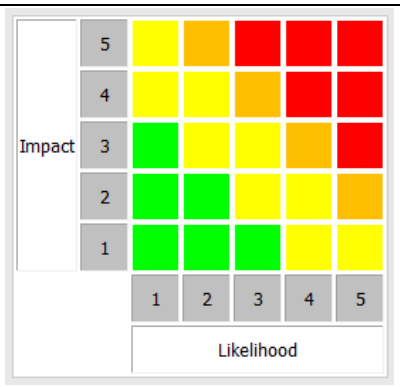


Figure 2 - Risk appetite

1.1.2.2 How to change the risk appetite

Individual cells within the risk matrix can be modified by clicking on the cell which will cause the cell to cycle through the available colours.

1.1.2.3 Adding new colours

Click "Setup Colours" displayed on the appetite matrix screen (shown in Figure 2 - Risk appetite) and a list of configured colours is displayed as shown in Figure 3 - Risk colours. To modify a colour, click on a coloured box (highlighted blue in Figure 3 - Risk colours) and a "colour picker" panel will appear (highlighted red in Figure 3 - Risk colours). Choose a new colour by using the scale and clicking the required colour shade. This will then change the colour of this tab. To delete a colour click the "delete" link associated with that colour.

Note: Colours must be in ascending severity order.

Warning: Deleting colours is a firm delete operation.

Figure 3 - Risk colours

1.1.3 Organisation Threats

1.1.3.1 What are threats and threat types?

Threat types are collections of threats which are interrelated. A threat is a potential risk that has a given likelihood of causing an impact to an organisation. To ensure a consistent approach, threats are considered at an organisation level, and risk assessments that take place must use this list.

To view organisational threats, click on “RA Setup” from the main organisation homepage, then select “Organisation Threats”.

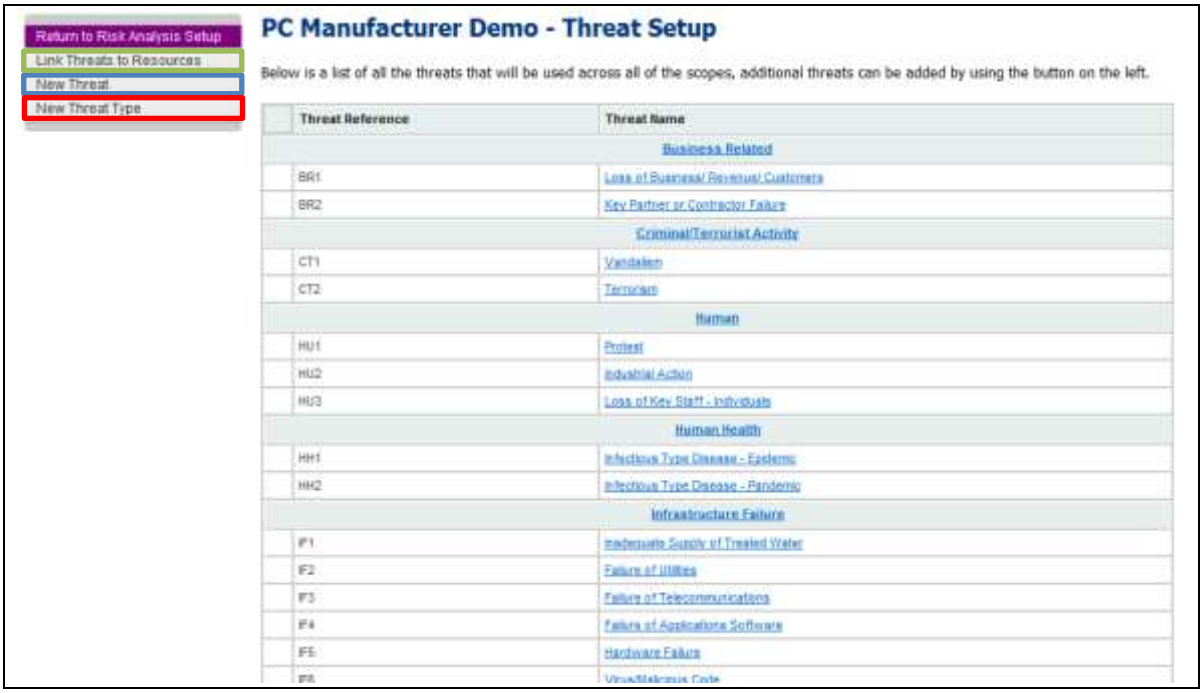


Figure 4 - Threat list

1.1.3.2 Adding new threat types

New threat types can be added by clicking on the "New Threat Type" link (highlighted red in Figure 4 - Threat list). Threat types are placeholders to group together threats and therefore only require a name.

1.1.3.3 Deleting threat types

Threat types can only be deleted when there are no threats attached to them. Click on a threat type that needs to be deleted and click "Delete Threat Type" from the left hand sidebar.

Warning: As a threat type can only be deleted when no threats exist, this is a firm delete operation.

1.1.3.4 Adding new threats

New threats can be added by clicking on the "New Threat" link (highlighted blue in Figure 4 - Threat list). As well as name, description and threat type, other attributes exist that need to be defined. Descriptions of each of these attributes are in Table 1 - Threat Attributes.

Threat Attribute Name	Description
Threat Reference	This is an organisation defined reference for the threat, there is not default but it is recommended that a logical naming scheme is used.

Duration Flag	Some threats could cause an impact more because they affect a resource for a time period that actually a direct impact. For example, within an office based business a power cut might cause very little direct impact but would render an office unusable. The impact can then be derived from the impact that was assessed during the BIA.

Table 1 - Threat Attributes

The threat entry form is shown within Figure 5 - Threat form.

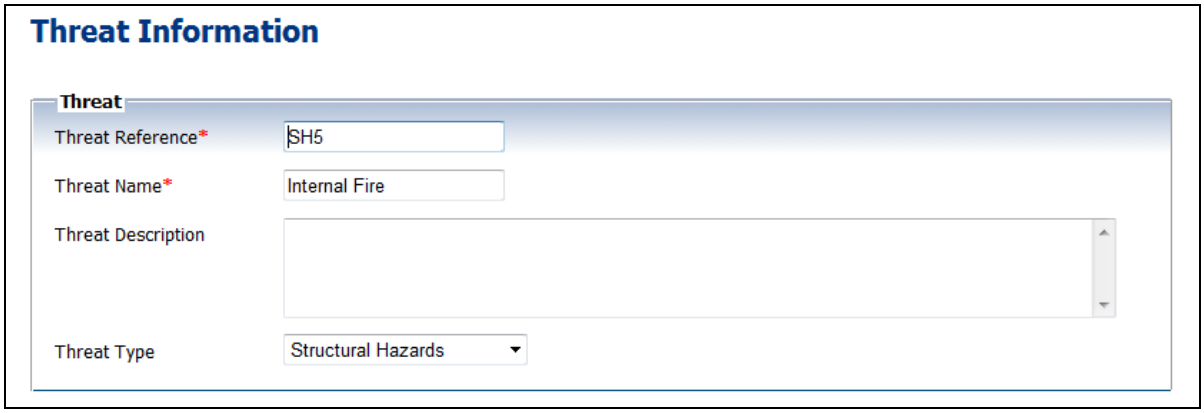


Figure 5 - Threat form

1.1.3.5 Threat to resource mapping

Different threats only affect certain types of resources. For each threat that is entered into Abriska, it must be linked to each of the default resource types. This linking is shown within Figure 6 - Threat to resource mapping. To access this list, click on the "Link Threats to Resources" link as highlighted green in Figure 4 - Threat list.

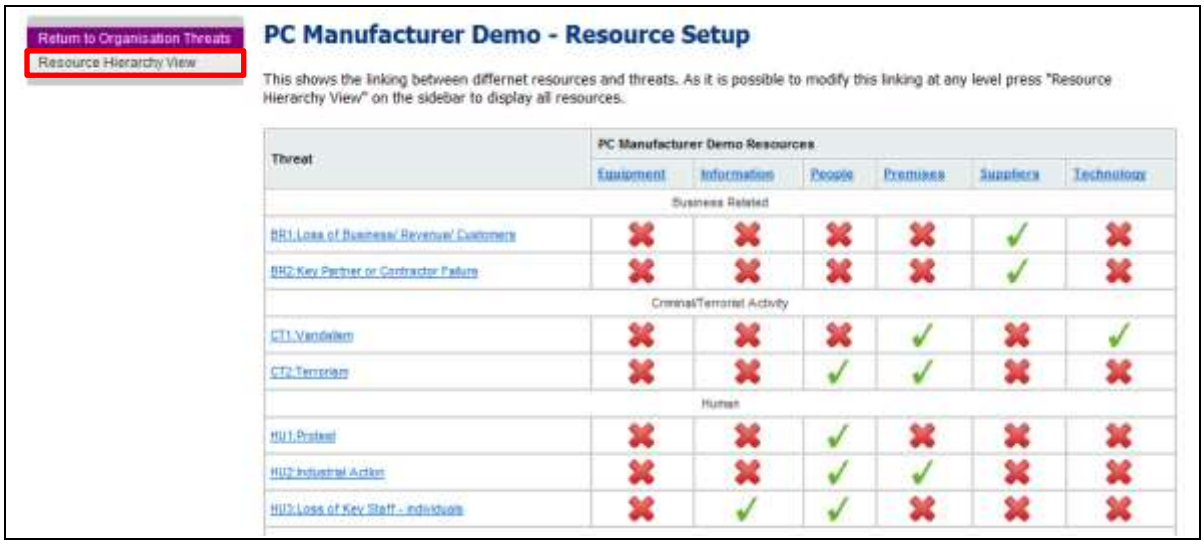


Figure 6 - Threat to resource mapping

For each of the default resource categories (People, Premises etc.), a tick or cross will be shown against each threat. To edit this mapping, click on the category name at the top (Equipment, Information etc) and a form listing organisation threats will be displayed. Tick the checkboxes next to the required threats and "Submit".

Warning: This will delete the existing mapping and could therefore affect any risk assessment that has already been conducted. This is a firm delete operation.

1.1.3.6 Resource threat linking hierarchy

To allow an additional level of granularity to be added to this relationship, individual resources or resource sub-categories can have a customised threat linking. From the "Resource Threat Linking" page, click on the "Resource Hierarchy View" (highlighted red in Figure 6 - Threat to resource mapping). The resource hierarchy will be displayed (shown in Figure 7 - Customising the threat to resource mapping hierarchy).

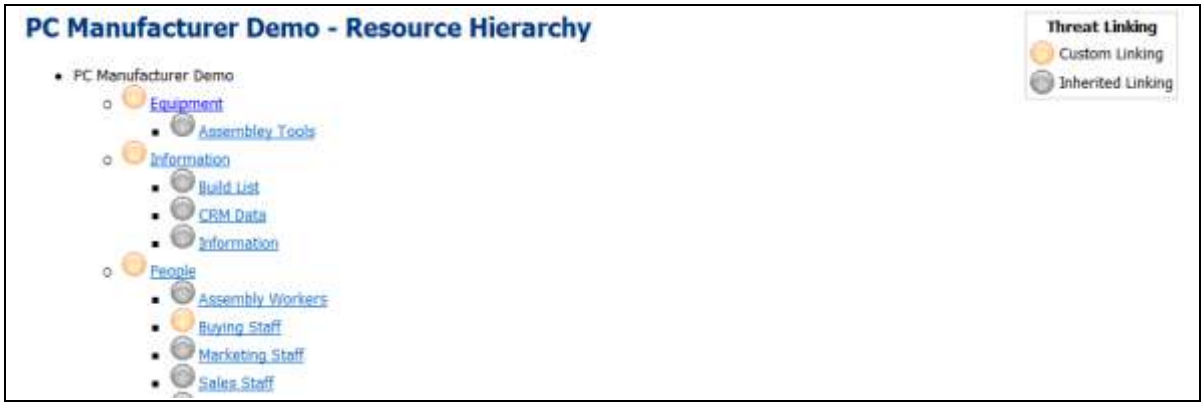


Figure 7 - Customising the threat to resource mapping hierarchy

If a resource is modified to have a unique threat mapping, any child resource of that resource will inherit the parent's customised mapping.

1.1.3.7 Threat to control mapping

If a risk assessment is being used in conjunction with the control maturity assessment, each threat needs to be linked through to one or more controls. This mapping indicates that the chosen control helps to mitigate a threat by reducing its vulnerability. If no controls are linked to a threat, an error will be highlighted in red.

1.1.3.8 Threat attributes

If the impact variable is setup to calculate risk against the organisation attributes (i.e. Confidentiality, Integrity and Availability). The default values can be assigned at an organisation level. If values are assigned at this level, these will become default for each entity risk assessment unless specified at a division level.

2.0 Conducting a risk assessment

The risk assessment focuses on the risks that are associated with a resource, and then links these risks to an activity that uses these resources. This allows a risk to be raised against a single resource but for it to map onto all of the activities that use it, this reduces the repeating of information.

Multiple risk assessments can be created and managed within Abriska. To allow groups of resources to be included within risk assessments, the concept of an "Entity" is used. An "Entity" is a risk assessment conducted against one or more groups of assets. For example, this could be all resources which from a single site, or all resources which are used by an activity, or just all resources that a are part of a single contact.

Figure 8 - List of entities

To view the organisations risk assessments, click on "Entities" from the organisation homepage. To modify the name, description, or to assign this entity to a contact, click on the entity name (highlighted red in Figure 8 - List of entities) then click "Setup Entity".

2.1 Entity Risk Assessment Flow

Abriska guides the users through an organisation defined workflow that meets the requirements of BS 25999. The default workflow is shown in Figure 9 - Activity flowchart.

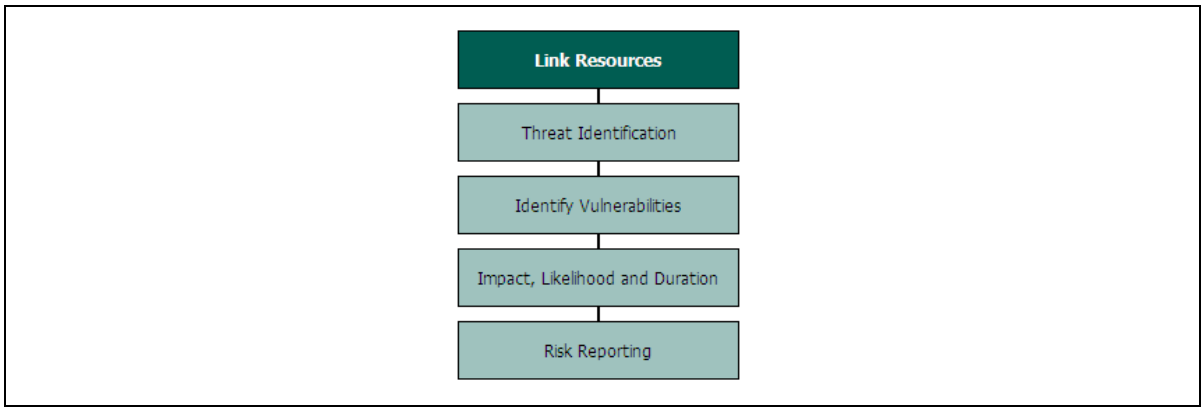


Figure 9 - Activity flowchart

The links available on the sidebar will increase depending on the work stage. All of the buttons that are available are shown within Figure 10 - Expanded entity sidebar.

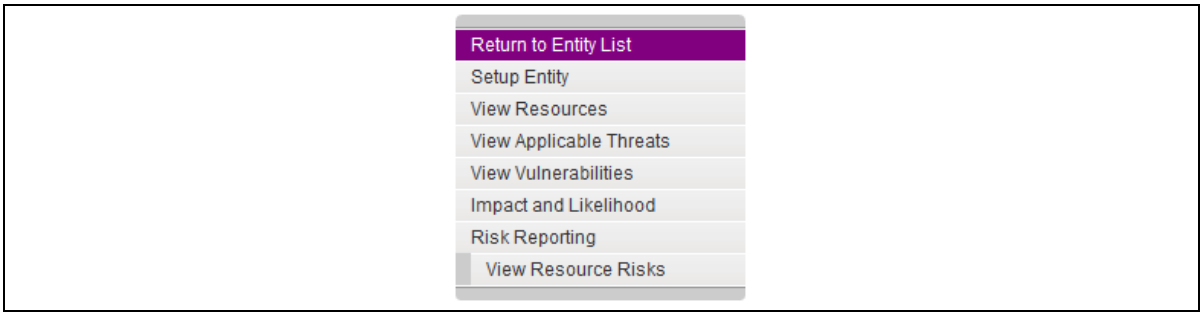


Figure 10 - Expanded entity sidebar

2.2 Identify resources

Resources need to be allocated to each entity to perform a risk assessment. Resources can be allocated to more than one entity to allow central resources to be included throughout organisation risk assessments.

To select resources for an entity, click "View Resources" after clicking the entity name (highlighted red in Figure 8 - List of entities). All available resources will be displayed with a filter to allow resources to be filtered by division. Select those that need to be included within this risk assessment by clicking the checkbox next to each resource name (highlighted red in Figure 11- Identifying resources).

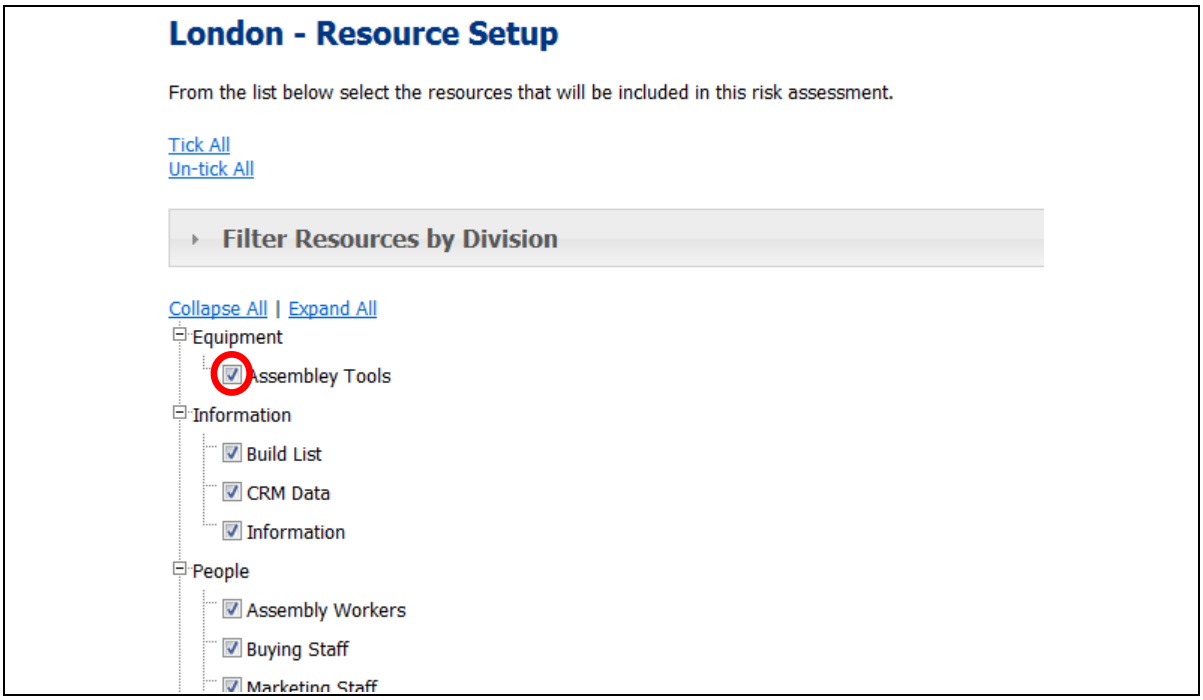


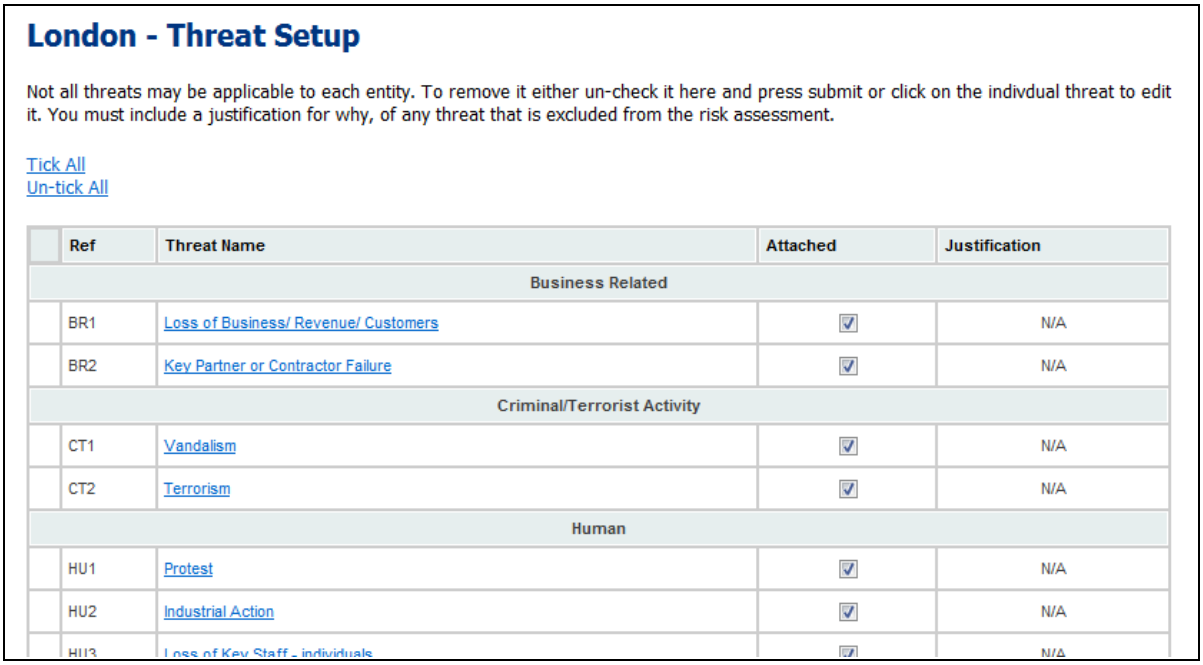
Figure 11- Identifying resources

Note: If resources are added after the risk assessment has been started, Abriska will require that each threat that is related to the newly added resources is reviewed.

2.3 Threat identification

To enforce a level of consistency across each risk assessment that is conducted using Abriska, the same organisation threats list is considered each time. If one of the organisation threats is not applicable to a risk assessment (either it is outside of the scope of the assets/resources within the review or it is not a realistic threat) it can be excluded from the entity. To exclude a threat a justification must be provided.

If a threat is outside those that are linked to a resource associated with this entity, a default justification will be entered into these threats. If a threat is added that is not linked to any of the resources (see section 1.1.3.5 Threat to resource mapping), the threat will be highlighted red, as will the flowchart stage.



London - Threat Setup

Not all threats may be applicable to each entity. To remove it either un-check it here and press submit or click on the indivdual threat to edit it. You must include a justification for why, of any threat that is excluded from the risk assessment.

Tick All
Un-tick All

	Ref	Threat Name	Attached	Justification
		Business Related		
	BR1	Loss of Business/ Revenue/ Customers	☑	N/A
	BR2	Key Partner or Contractor Failure	☑	N/A
		Criminal/Terrorist Activity		
	CT1	Vandalism	☑	N/A
	CT2	Terrorism	☑	N/A
		Human		
	HU1	Protest	☑	N/A
	HU2	Industrial Action	☑	N/A
	HU3	Loss of Key Staff - individuals	☑	N/A

Figure 12 - Justify non-applicable threats

Note: If additional threats are added at any point, they will appear in this threat list and the risk assessment will be marked as not complete. The reason for this is newly identified organisational threats may need to be considered for this risk assessment.

2.4 Identify vulnerabilities

A vulnerability is:

"*A weakness in a resource or group of resources that can be exploited by one or more threats*"

Individual vulnerabilities need to be identified that might increase the organisation's exposure to certain threats,

Figure 13 - Vulnerability list

2.4.1 Adding vulnerabilities

Vulnerabilities can only be modified when the vulnerability assessment is unlocked. To do this, click "Modify the Vulnerability Assessment" (highlighted red in Figure 13 - Vulnerability list). Additional vulnerabilities can now be added by clicking the "Add vulnerability" link. Vulnerabilities can also be added from the Abriska "Vulnerability Library" which contains template examples of vulnerabilities. Once all of the vulnerabilities have been added, to progress onto the next stage of the risk assessment, click "Complete Vulnerability Assessment" (highlighted blue in Figure 14 - Vulnerability list – alternative buttons).

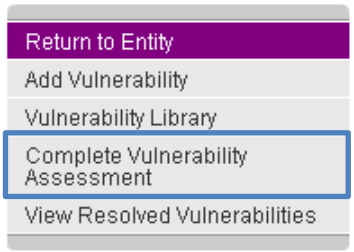


Figure 14 - Vulnerability list – alternative buttons

When initially adding a vulnerability, only the name and description fields are required. The reference will be automatically generated by Abriska depending on the next available reference number. Once a vulnerability is added, it needs to be classified in terms of vulnerability type, what resources it is linked to, and which threats it affects. Each of these attributes is covered in the following sections.

Note: After a new vulnerability is added, each threat that is linked to it must be reviewed.

2.4.2 Vulnerability type

Each vulnerability could affect an organisation's resources in a different way. It could be a combination of the factors described in Table 2 - Vulnerability type attributes.

Vulnerability Type	Description
Increase likelihood	The resources that are affected by this vulnerability are more likely to be affected by the threats that this vulnerability is linked to. For example, if an organisation's HQ is located on a flood plain then there is a higher chance of flooding.
Increase impact	Due to this vulnerability, the impact on the organisation would be greater. For example, if a single point of knowledge exists within a worker, there would be an increase impact of the threat loss of key staff.
Increase duration	Due to this vulnerability the time to recover the related resources after an incident is increased. For example, if specialised/unique equipment is used within a process then if this fails there will be added increased time to recover.

Table 2 - Vulnerability type attributes

Types are entered against each vulnerability under the "Types" tab (shown in Figure 15 - Vulnerability types).

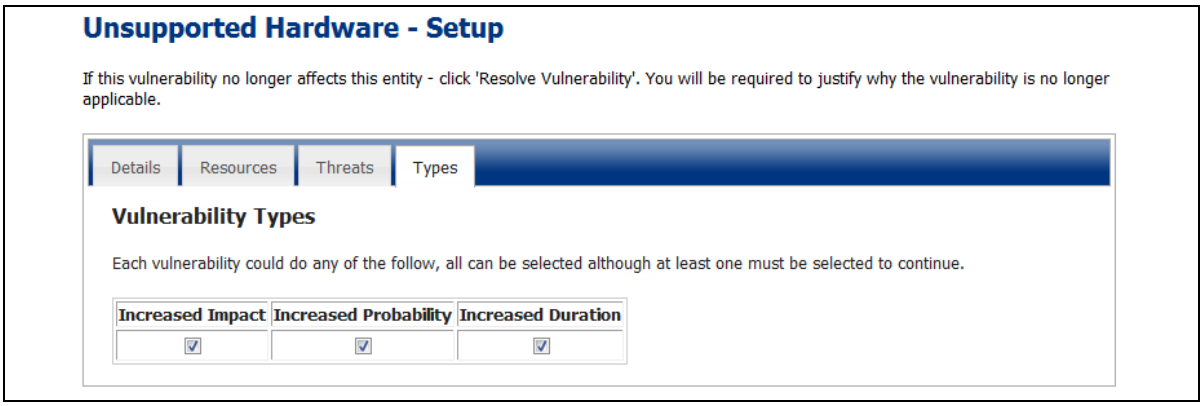


Figure 15 - Vulnerability types

2.4.3 Linking vulnerability to resources

Each vulnerability needs to be linked to at least one resource. This is achieved via a hierarchy of assets that are linked to this entity.

Figure 16 - Linking vulnerability to resources

Resources are linked to each vulnerability via the "Resources" tab (shown in Figure 16 - Linking vulnerability to resources).

2.4.4 Linking vulnerability to threats

Each vulnerability needs to be linked to at least one threat. This is achieved by selecting from those threats that are applicable to this entity.

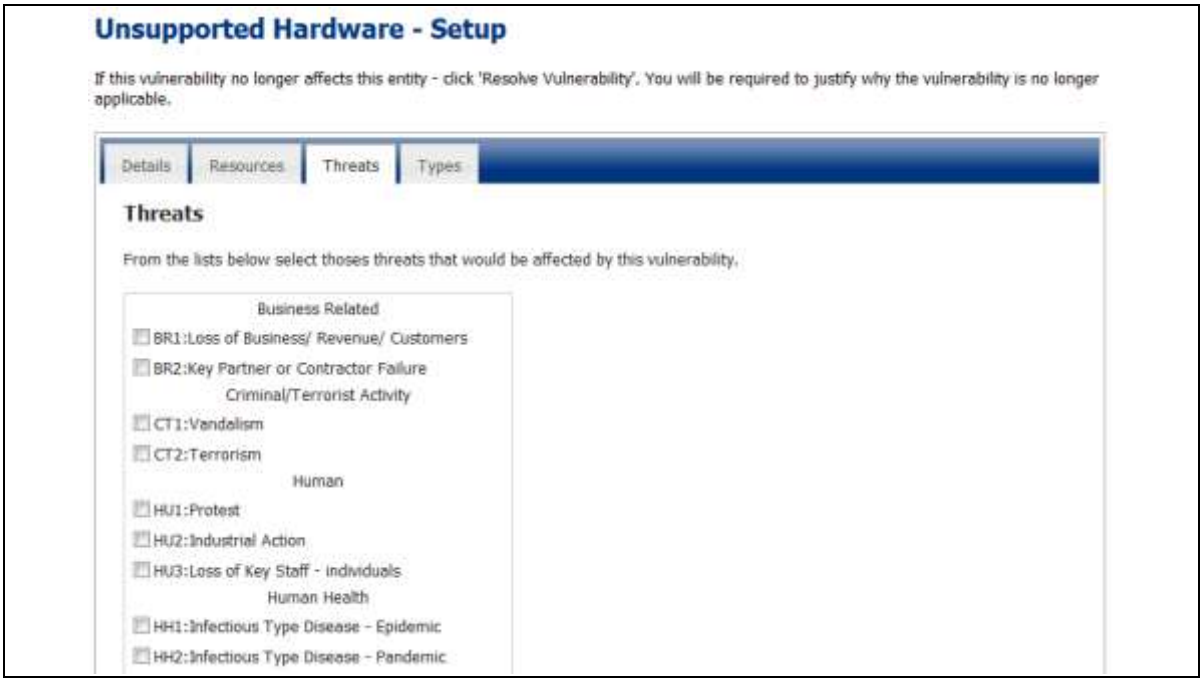


Figure 17 - Linking vulnerability to threats

Resources are linked to each vulnerability under the "Resources" tab (shown in Figure 17 - Linking vulnerability to threats).

2.5 Impact, likelihood and duration

For every threat that is applicable to the entity, each of the risk variable and the duration (if applicable) need to be evaluated. From the main entity screen shown in Figure 8 - List of entities, click on the "Impact and Likelihood" link and screen in Figure 18 - Threat List will be displayed.

Figure 18 - Threat List

Each threat must be evaluated singularly by clicking on the threat name which will display the threat risk form shown in Figure 19 - Individual threat showing specific tabs.

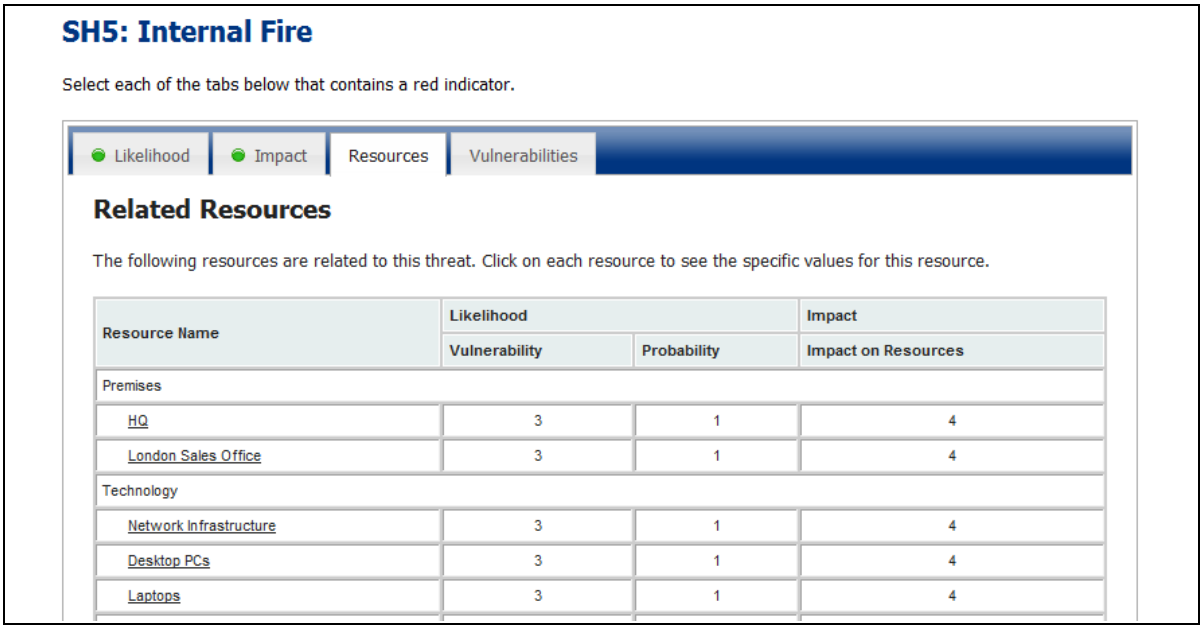


Figure 19 - Individual threat showing specific tabs

Each of the resources that are linked to this threat will be displayed on the "Resources" tab (shown in Figure 19 - Individual threat showing specific tabs). For each of the risk variables specified in 1.1.1 Risk Variables, a tab will appear that allows each of the variables to be quantified. A red indicator on the tab shows that the section is unanswered which changes to green once this is answered.

For each of the variables selected, identify the value that best fits with this threat. When considering the likelihood and impact of the threat, take into account the vulnerabilities that are also attached to that threat.

Figure 20 - Entity threat variable

Note: A history of all answers which have been provided or changed are available by clicking the "View Variable History" button.

2.6 Quantifying a vulnerability

If the threat that is being reviewed has any vulnerabilities related to it, an additional tab will display - "Vulnerabilities". This tab will show all of the vulnerabilities within an expanding list shown in Figure 21 - Quantifying . This allows an organisation to alter how a particular threat relates to a certain resource.

As an example, suppose Figure 21 - Quantifying . Rather than rate all of the resources within the entity as being a single point of failure, the value can be overwritten for the resources affected by this vulnerability.

Figure 21 - Quantifying vulnerability

2.7 Addressing a vulnerability

When a specific vulnerability is addressed by an organisation, it could be that a control has been put in place to mitigate the effect of a vulnerability, or because working practices have been changed. Select a vulnerability that has been addressed and click "End Date Vulnerability". This allows a justification to be provided and the vulnerability will no longer be visible within the vulnerability list.

Note: After a vulnerability is addressed, each threat that is linked to it must be reviewed. This is because risk of that threat is now lower.

Appendix A. List of figures