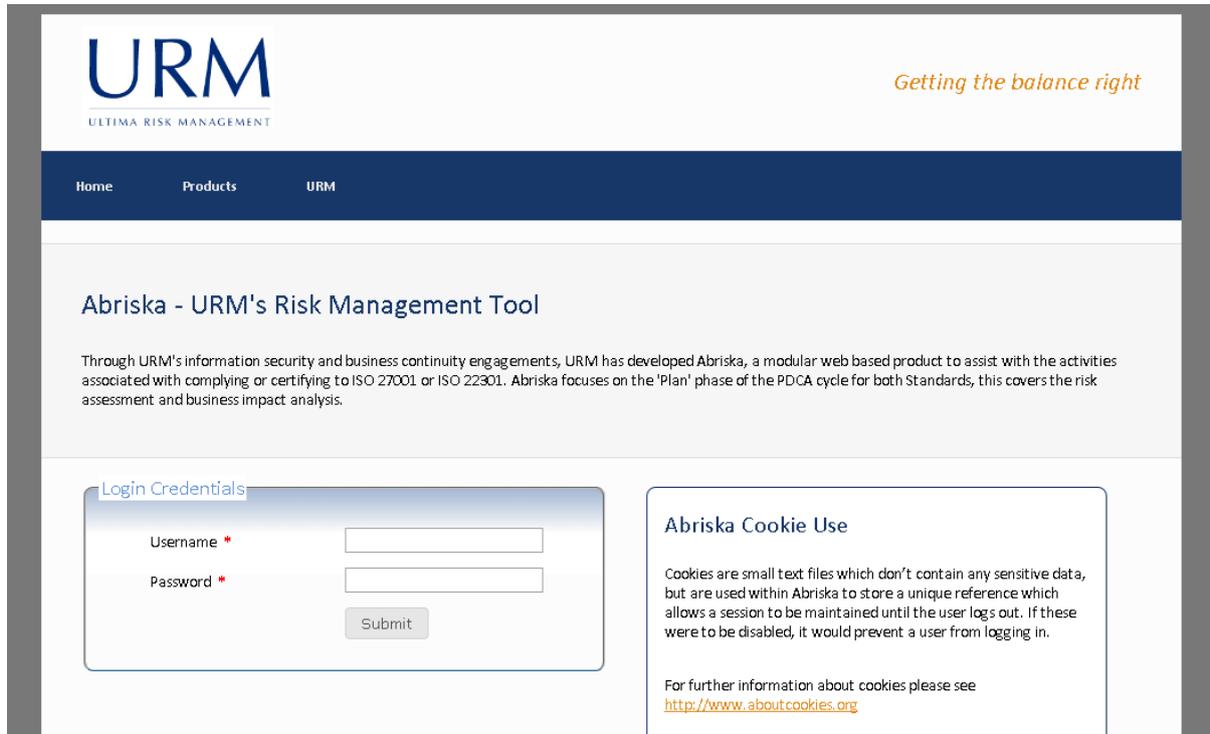
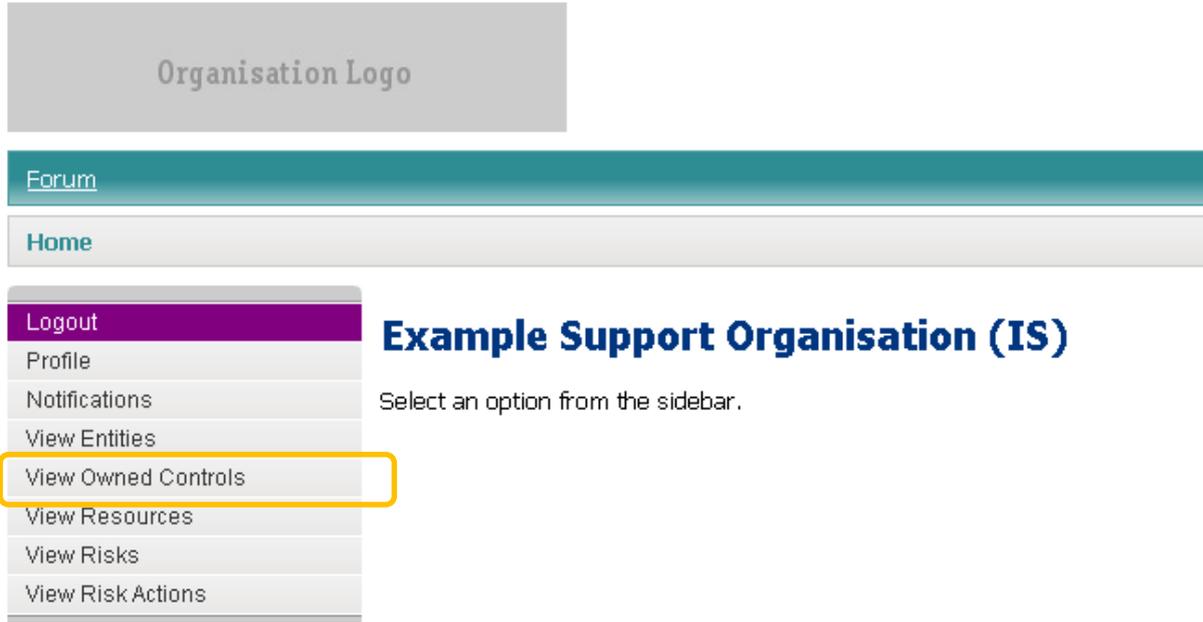


Abriska is access online via <https://www.abriska.com>, your username is your email address and your password will have been sent via email.



Upon Logging in you'll be presented with a screen that looks like this:



Click on View Owner Controls, highlighted orange above.

Organisation Logo

Forum

Contact Division

Return to Home

## Divisions

Division Name	Number of Controls	Available Actions
Example Support Organisation (IS)	7	<div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px; background-color: #f0f0f0;">Example Support Organisation (IS) Control Assessment</div> <div style="border: 1px solid #ccc; padding: 5px; background-color: #f0f0f0;">Example Support Organisation (IS) Control Risk Strategies</div>

The above page displays the two options that are available for controls. Initially, click on the “... Control Assessment” button.

### Example Support Organisation (IS) - Controls

Control Group	Control Reference	Control Name	Owner	Maturity Defined and Justified	Proposed Maturity Defined and Justified
<span style="background-color: orange; width: 15px; height: 15px; display: inline-block;"></span> ISO 27001	5.1.1	<a href="#">Policies for information security</a>	Basic User	1:Initial/Ad Hoc	4:Managed and Measurable
<span style="background-color: orange; width: 15px; height: 15px; display: inline-block;"></span> ISO 27001	5.1.2	<a href="#">Review of the policies for information security</a>	Basic User	3:Defined Process	4:Managed and Measurable
ISO 27001	6.1.1	<a href="#">Information security roles and responsibilities</a>	Basic User	2:Repeatable but Intuitive	4:Managed and Measurable
ISO 27001	6.1.2	<a href="#">Segregation of duties</a>	Basic User	1:Initial/Ad Hoc	4:Managed and Measurable
ISO 27001	6.1.3	<a href="#">Contact with authorities</a>	Basic User	2:Repeatable but Intuitive	4:Managed and Measurable
			Basic	4:Managed and Measurable	4:Managed and Measurable

This will display a list of controls which need to be reviewed. Some controls may have a coloured indicator next to them, which is explained by a key on the right of the screen (not displayed above). Click on the control name to review and edit this item. If there are any controls which you believe you do not own please contact your organisation administrator.

### 5.1.1: Policies for information security

**Description:** A set of policies for information security shall be defined, approved by management, published and communicated to employees and relevant external parties.

Current Implementation
Recommendation
History
Graph
Documents

**Current Implementation**

Describe the current implementation of this control then state the maturity of this control at present.

Current Implementation

Answered By: User 1  
Answered Date: 26 Feb 2014 21:39:46:223

Maturity Name	Description	Radio
0:Non-existent	Complete lack of any recognisable processes. The organisation has not even recognised that there is an issue to be addressed.	<input type="radio"/>
1:Initial/Ad Hoc	There is evidence that the organisation has recognised that the issues exist and need to be addressed. There are, however, no standardised processes; instead, there are ad hoc approaches that tend to be applied on an individual or case-by-case basis.	<input type="radio"/>
2:Repeatable but Intuitive	Processes have developed to the stage where similar procedures are followed by different people undertaking the same task. There is no formal training or communication of standard procedures, and responsibility is left to the individual. There is a high degree of reliance on the knowledge of individuals and, therefore, errors are likely.	<input type="radio"/>
3:Defined Process	Procedures have been standardised and documented, and communicated through training. It is mandated that these processes should be followed; however, it is unlikely that deviations will be detected. The procedures themselves are not sophisticated but are the formalisation of existing practices.	<input type="radio"/>
4:Managed and Measurable	Management monitors and measures compliance with procedures and takes action where processes appear not to be working effectively. Processes are under constant improvement and provide good practice. Automation and tools are used in a limited or fragmented way.	<input type="radio"/>
5:Optimised	Processes supporting this control have been refined to a level of good practice, based on the results of continuous improvement. Security is used in an integrated way to automate the workflow, providing tools to improve quality and effectiveness, making the organisation quick to adapt.	<input type="radio"/>

**Controls Navigation**

5.1.2 ▶

Save

Describe how the control is currently implemented within the 'current implementation' tab and evaluate the current maturity (select the current maturity using the radio button to the right of the page, highlighted orange above). If there are any recommendations for how this control can be improved, click the 'recommendation' tab and a similar page will display.

Current Implementation
Recommendation
History
Gr

**Recommended Improvement**

Describe a proposed improvement for this control then state the implemented.

Recommendation

Proposed Implementation Date

Additionally a proposed implementation date can be recorded for when this recommendation can be implemented. An email reminder will be sent out ahead of this date and also once this date has passed. Once all controls are assessed, navigate back to the view owned controls (shown at the top of page 2 of this guide).

Click on the “... Control Risk Strategies” button. This time all of the controls will display, however they will be in a priority order based on the interrelationships within Abriska.

### Example Support Organisation (IS) - Controls

Below are all of the controls that have been assessed within this division. The risk scores are the maximum current risk associated with controls. A risk strategy can be selected for each risk that is identified.

Control Group	Control Reference	Control Name	Max Risk Indicator	Risk Strategy
ISO 27001	5.1.1	Policies for information security	18.5	-
ISO 27001	6.1.2	Segregation of duties	18.5	-
ISO 27001	6.1.1	Information security roles and responsibilities	15.5	-
ISO 27001	6.1.3	Contact with authorities	15.5	-
ISO 27001	6.1.5	Information security in project management	15.5	-
ISO 27001	6.1.2	Review of the policies for information security	15.5	-

Click on each control name in turn:

	Inherent	Controlled	Treated
Max Risk Score	20	18.5	7.25
Maturity Level	0:Non-existent	1:Initial/Ad Hoc	4:Managed and Measurable
Maturity Description	Complete lack of any recognisable processes. The organisation has not even recognised that there is an issue to be addressed.	A policy has been drafted but not yet signed off or published. Last updated by: User 1 @ 26 Feb 2014 21:39:46:223	Proposed Date:30 Apr 2014 00:00:00:000 SMT to sign off and publish. Last updated by: User 1 @ 26 Feb 2014 21:39:46:223

**Risk Strategy**

Risk Treatment Decision\*

Risk Treatment Owner\*

Risk Review Date\*

**Risk Actions**

There is no treatment action associated with this risk.

Abriska displays three levels of risk:

- Inherent/Absolute – the risk if no controls were in place
- Controlled/Current – the current level of risk
- Treated/Residual – the estimated level of risk should improvements be made to the controls.

The risk treatment decision, next review date and owner should be selected and the results of this submitted, highlighted orange above.

If individuals or teams are required to perform actions to enable this risk treatment to be effectively implemented, the actions can be created, tracked and managed through Abriska.

The screenshot shows a web interface titled "Risk Actions". At the top, it states "There is no treatment action associated with this risk." Below this are two buttons: "New Action" and "Resolved Actions". The "New Action" button is highlighted in orange. Below the buttons is a form titled "New Risk Action Setup" with a close button (x) in the top right corner. The form contains the following fields:

- "Risk Treatment Action": A text input field.
- "Action Owner": A dropdown menu with a dashed line indicating a selection.
- "Proposed Date": A date input field.
- "Submit": A yellow button.

Additional details about other functionality is available within the online user guide within the top right of Abriska (highlight orange below).

