URM

ULTIMA RISK MANAGEMENT

# Abriska:
# Control Maturity Assessment

## User Guide

Ultima Risk Management Limited

# Abriska

## 1.0 Introduction

The control maturity assessment allows individual controls to be added to the organisation and assessed against a maturity model. This assessment allows weaknesses within controls to be identified and improvements against controls defined.

This assessment is used to calculate how vulnerable a resource is to a particular threat (highlighted blue within the diagram below Figure 1 - Risk Diagram).

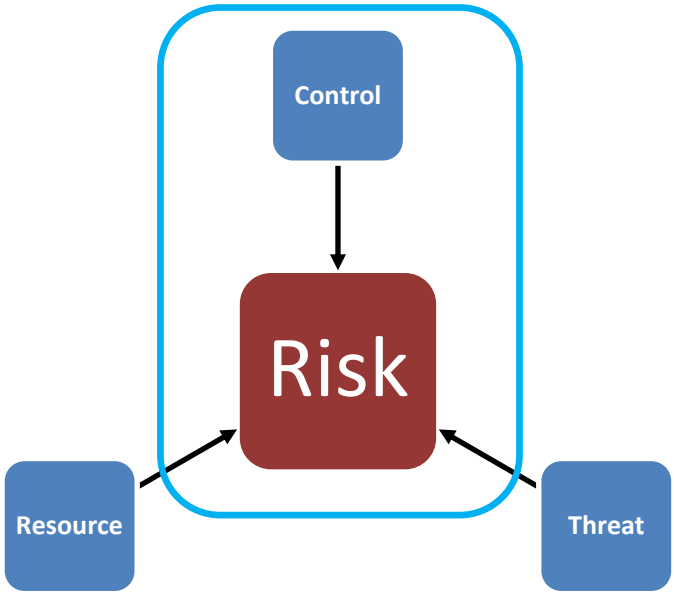


**Figure 1 - Risk Diagram**

# 2.0 Control maturity assessment setup

## 2.1 Control maturity assessment setup

To access the following control maturity assessment setup screens, navigate to the organisation home and click “CMA Setup”.

## 2.2 Maturity Model

### 2.2.1 What is the maturity model?

To determine how well each of the controls has been implemented within the organisation a standard set of criteria needs to be defined, Abriska uses a maturity model to define these criteria. This also enforces a level of consistency across the control maturity assessment.

The maturity model is a graded scale that allows a controls implementation to be assessed and given an effectiveness level. For example, Figure 2 - Control Maturity shows how the effectiveness of a control would vary depending on the maturity that has been assigned.

**Demo Organisation - Maturity Model**

| Maturity Model Name | Description | Levels | | | | | |
|---|---|---|---|---|---|---|---|
| ISO 27001 Control Maturity | | 0\|Non-existent | 1\|Initial/Ad Hoc | 2\|Repeatable but Intuitive | 3\|Defined but not effective | 4\|Managed and Measurable | 5\|Optimised |

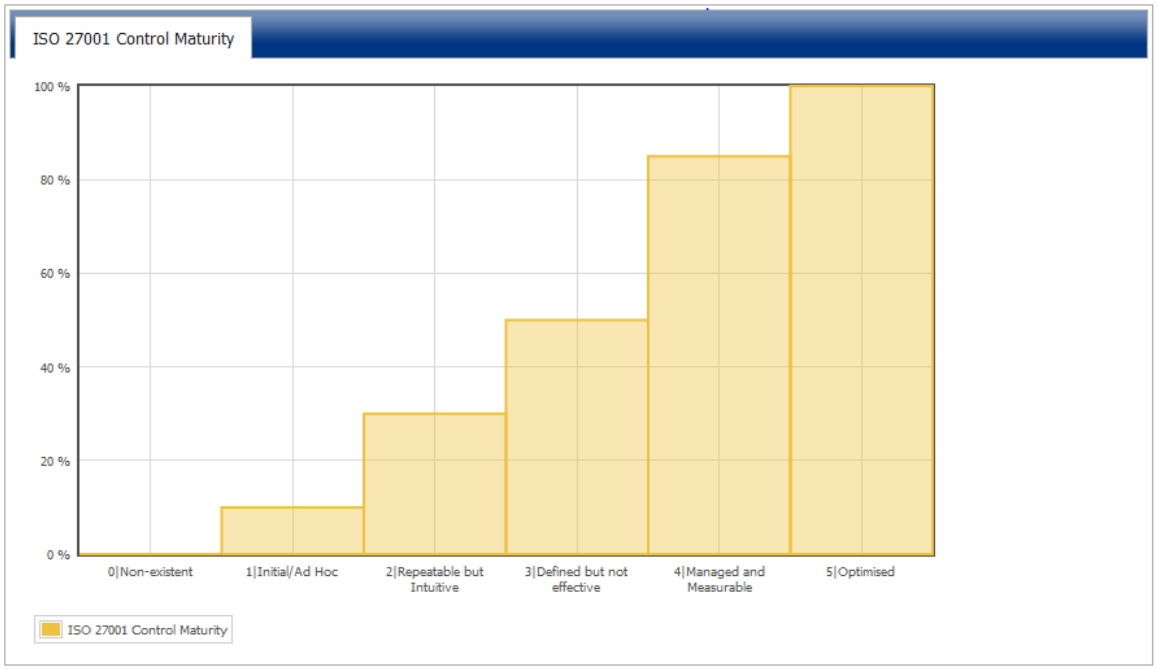


**Figure 2 - Control Maturity**

**Note:** multiple maturity models can exist for different control areas and also different numbers of levels can be defined.

### 2.2.2 The default maturity model

By default, Abriska comes pre-loaded with a maturity model that has been defined for ISO 27001. This maturity model is based on the industry Standard (Control Objectives for Information and related Technology (COBIT®) - IT Governance Institute). There are six levels within the maturity model ranging from level 0 (Non-existent) through to level 5 (Optimised) and each level as a defined effectiveness.

## 2.3 Controls

These are include all policies, processes, procedures, organizational structures and technical controls that could be selected and implemented to ensure risks are reduced to an acceptable level. If using Abriska to conduct an ISO 27001 assessment the controls within ISO 27001 Annex A are included within Abriska.

All controls within Abriska need to be allocated to a control group, this allows control sets to be grouped together i.e. ISO 27001 or APACS 55.

### 2.3.1 Control to Threat Linking

Each control that is loaded into Abriska needs to be related through to the threats that they mitigate. This relationship is used within the risk calculation to calculate how vulnerable a resource is to a particular threat.

For example, consider the risk of computer viruses and malicious code, potential controls that could be implemented include having anti-virus controls and awareness training. If either of these controls is weak then the organisation's resources could be vulnerable to virus / malicious code.

 **Warning:** Changing the control to threat linking will modify the results of the risk assessment.

### 2.3.2 Control to Resource Linking

Each control that is loaded into Abriska also needs to be related through to the resources that they protect. This relationship is used within the risk calculation to calculate how vulnerable a resource is to a particular threat.

By default the relationships are all set to true, therefore each control can potentially reduce the vulnerability of all resources. These setting can be configured when an organisation wishes to conduct a very detailed risk assessment of a certain asset type (for example, paper assets).

 **Warning:** Changing the control to resource linking will modify the results of the risk assessment.

### 2.3.3 Control Groups

Control groups are collections of controls. The default group is ISO 27001. Additional control groups can be created for extra control sets that are added to Abriska.

# 3.0 Conducting a CMA

## 3.1 Assessing controls against the "root" division

Controls are assesses against any division within the organisations hierarchy. If a division is assessed then it will either be green or tan, if the control is not assessed at this level it will be indicated with a grey button.

This allows different areas of the organisation to have a different level of control maturity, for example, Figure 3 - Division control maturity assessment, shows a demo organisation whereby the overall organisation has been assessed but the support division has specific control (maybe additional controls around screening).

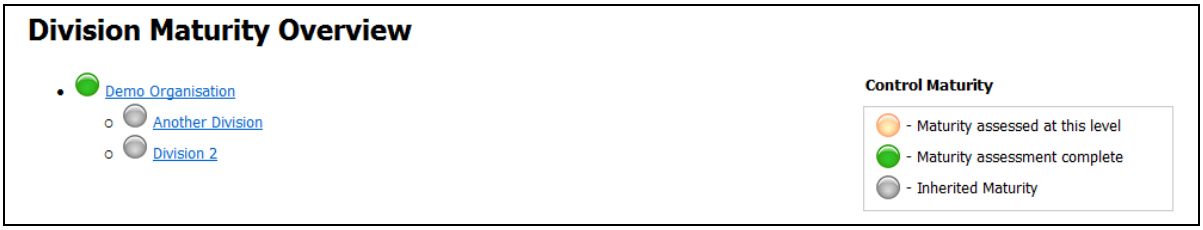


**Figure 3 - Division control maturity assessment**

### 3.1.1 Non-applicable controls

All controls that have been setup within the organisation will be defaulted in and will be applicable to this division; however some of the controls may not be applicable to a specific division / organisation. These can then be excluded from the assessment and any justification given will appear on the Statement of Applicability.

## 3.2 Assessing controls against an "inherited" division

### 3.2.1 Control Inheritance

For each of the sub divisions the option is given to either inherit the control maturity or specify it specifically at this level. This can be used when a specific sub division requires a control to be implemented to a far higher level.

| Control Status | Indicator | Description |
|---|---|---|
| **Inherited** |  | The maturity of this control is assessed at a divisional level higher than this division; therefore the maturity does not need to be assessed. |
| **Inherited Not Applicable** |  | This control is not applicable at a divisional level higher than this division so it not applicable at this division either. |
| **Assessed at this division level** |  | The maturity of this control needs to be assessed at this division. |

| Control Status | Indicator | Description |
|---|---|---|
| **Not applicable at this level** |  | This control is not applicable at this level (regardless of how this control has been assessed at other level.) |

### 3.3 Assigning Control Owners

Applicable controls can be assigned an owner. This allows an individual contact within Abriska who has been granted the "Basic User" role to logon and assess the maturity of that control. Controls can either be assigned an owner individually (by clicking on each control shown in Figure 4 - Applicable Control) or multiple controls can be assigned to a single contact via "Assign Control Owners".

### 3.4 Assigning other contacts to a control

Only a single contact can be defined as the control owner however additional contacts can be granted access to answer maturity questionnaires by clicking on the control within the control applicability, then clicking "Assign Contacts to Control". This will then allow a basic user access to assess this control without changing the control owner.

### 3.5 Control Status & Third Party

For each control the option exists to record the current implementation status of this control, the three values available by default are "Fully", "Partially" or "None". The reason for this is whilst undertaking certification to ISO 27001 a control, such as 7.2.1 Classification guidelines, may well be well documented within the management system but is not fully implemented within the organisation (for example, documents might exist that do not have a classification). This drop down allows that status to be recorded, this is reported on the Statement of Applicablility.

The "Transferred to 3rd Party" flag allows the control to be recorded as being implemented by a third party.

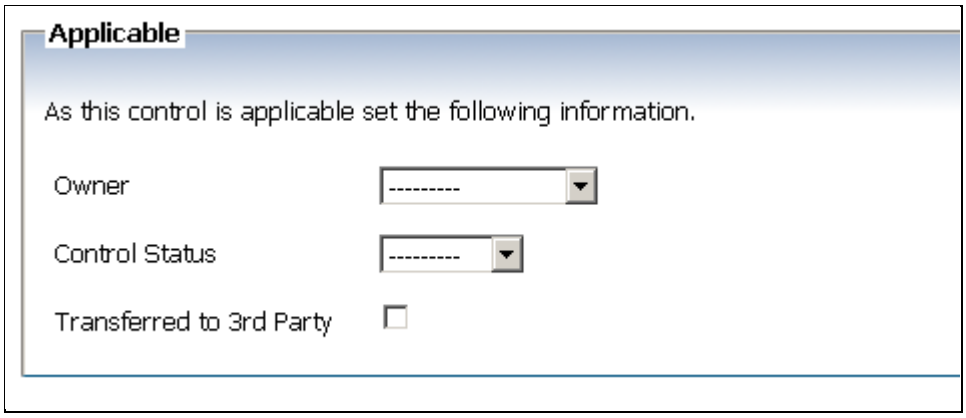


**Figure 4 - Applicable Control**

## 3.6 Control Maturity

Multiple tabs exist on the control maturity page, all tabs can be completed before submitting the page.

### 3.6.1 Current Implementation

Each applicable control needs to be assessed against the predefined maturity model. This should be completed by the control owner for that division and can either be completed by interview or assigned to that individual.

Navigation between controls is achievable by clicking on the forward / back navigation in the top right.

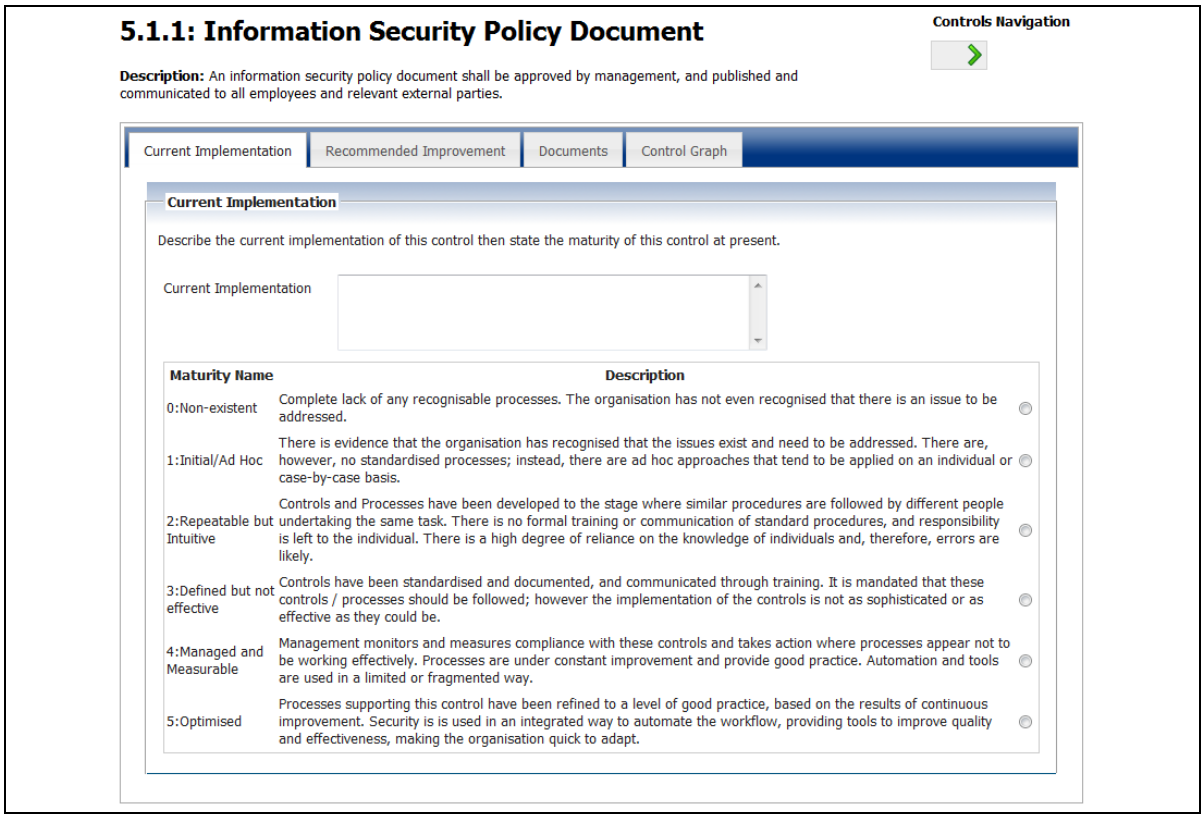


**Figure 5 - Assessing control maturity**

### 3.6.2 Recommended Improvement

Each control should be described and the maturity level for that control assigned within the current implementation tab. The recommended improvement tab can then be completed with a recommendation for how that control can be improved and a proposed maturity of that control should the recommendation be implement. There is also the opportunity to enter a proposed date for the recommendation. Figure 5 - Assessing control maturity shows the screen where the control maturity is assessed.

This recommendation will then be linked through to a related risk to ensure that the highest priority areas are addressed first.

**Note:** For controls where no recommendation is applicable a statement should be added that states how the control should be maintained and reviewed, the recommended maturity should also be set to the same level as the current maturity. This allow Abriska to calculate an expected risk score once the

### 3.6.3 Documents

There is also a tab within the maturity screen to link to related documents such as policies, procedures or documents that contain evidence. This allows the related documents to be loaded alongside the descriptions for how the control is currently implemented.

These document lists will also appear in the "Extended Statement of Applicability" and the "Risk Treatment Plan".

**Note:** Due to the security setting within the browser local links to resources such as file:/// will not open directly. To open these links either the security setting can be modified or the links can be copied and pasted.

## 4.0 Control Risk Strategies

The control risk strategy will only be completed after the resource attribute valuation (Confidentiality, Integrity and Availability), Control Maturity Assessment and the Risk Assessment entity are complete.

### 4.1 Divisions

This shows the maximum risk associated with each of the divisions

The tan indicator shows that the risk assessment or control assessment is still in progress so the results of the risk assessment are not yet visible.

### 4.2 Controls

This shows all applicable controls and the related risk score of that control, also displayed is the risk treatment action. Clicking on a control will populate the control overview tab and show the following information.

### 4.3 Control Overview

This shows the 3 values for risk:

| Risk Type | Description |
|---|---|
| **Absolute** | This value represents the score that would be achieved if the control was at the lowest level of maturity (by default 0: Non-existent). |
| **Controlled** | This is based on the current controls of the organisation |
| **Treated** | This is an estimated value based on the proposed maturity that was defined within the maturity assessment. |

**Note:** The names of these risk types can be modified for an organisation therefore these values may be different for your organisation. These can be modified within the Home -> Organisation -> RA Setup -> View Risk Types.

### 4.3.1 Risk Treatment Decision

A risk strategy can then be allocated to the controlled risk. The risk owner will be defaulted as the control owner but can be set as any contact within Abriska. An action description allows any difference from the recommendation to be recorded.

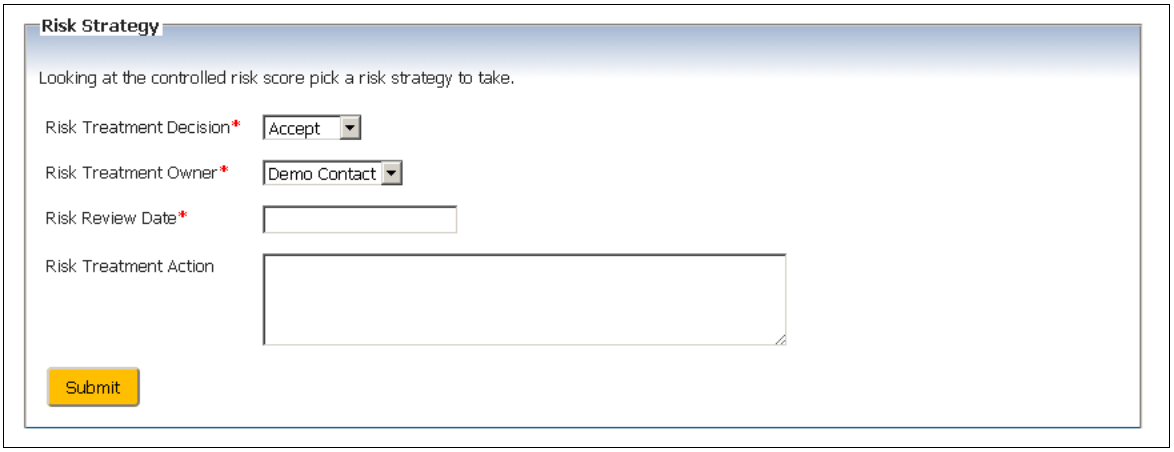


**Figure 6 - Risk Strategy**

The default risk decisions are explained below.

| Risk Treatment Decision | Description |
|---|---|
| **Accept** | Knowingly and objectively accepting risks, providing they clearly satisfy the organization's policy and criteria for risk acceptance.<br>I.e. Recommendation will not implemented. |
| **Avoid** | Avoiding risks by not allowing actions that would cause the risks to occur.<br>E.g. stop trading on the internet to avoid the risks associated with ecommerce. |
| **Reduce** | Applying appropriate controls to reduce the risks.<br>I.e. Implement the recommendation. |
| **Transfer** | Transferring the associated risks to other parties.<br>E.g. insurance or outsource. |

**Note:** The names of these risk treatment actions can be modified for an organisation therefore these values may be different for your organisation. These can be modified within Home -> Organisation -> RA Setup -> Risk Strategies.

## 4.4 Threats

This tab will only be populated once you click on the "Threat" button at the top of the control overview tab. It shows all of the threats that are related to this control, any therefore what threats the organisation is being exposed to having this control at this level of maturity. The maximum score on this table will be the maximum score for the control.

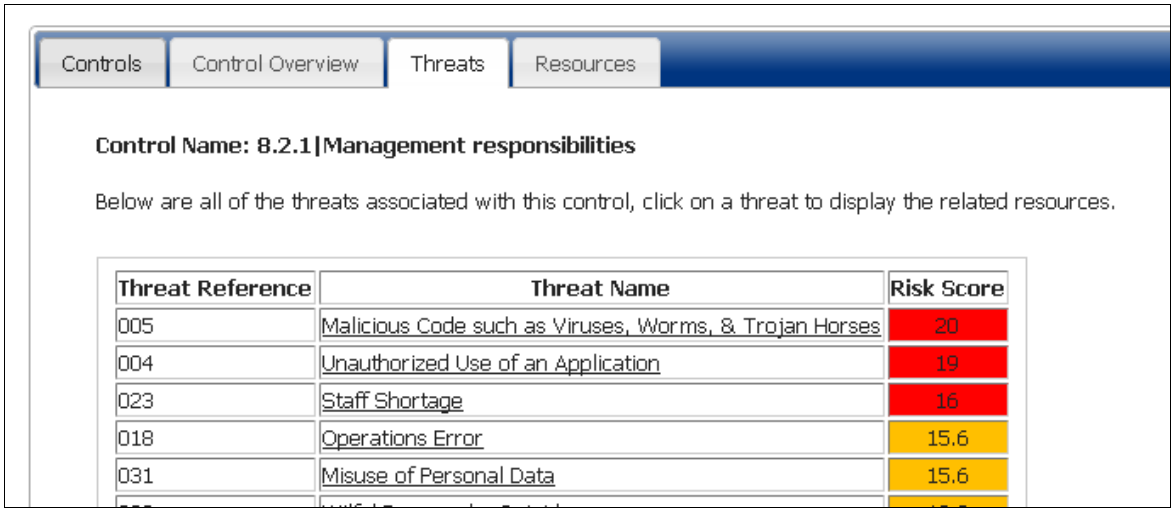


**Figure 7 - Related Threats**

## 4.5 Resources

This tab will only be populated once you click on the "Threat" button at the top of the control overview tab and then click on a threat and it will display all of the related resources. This will show all of the resources that are exposed to this threat as a result of the maturity of this control.

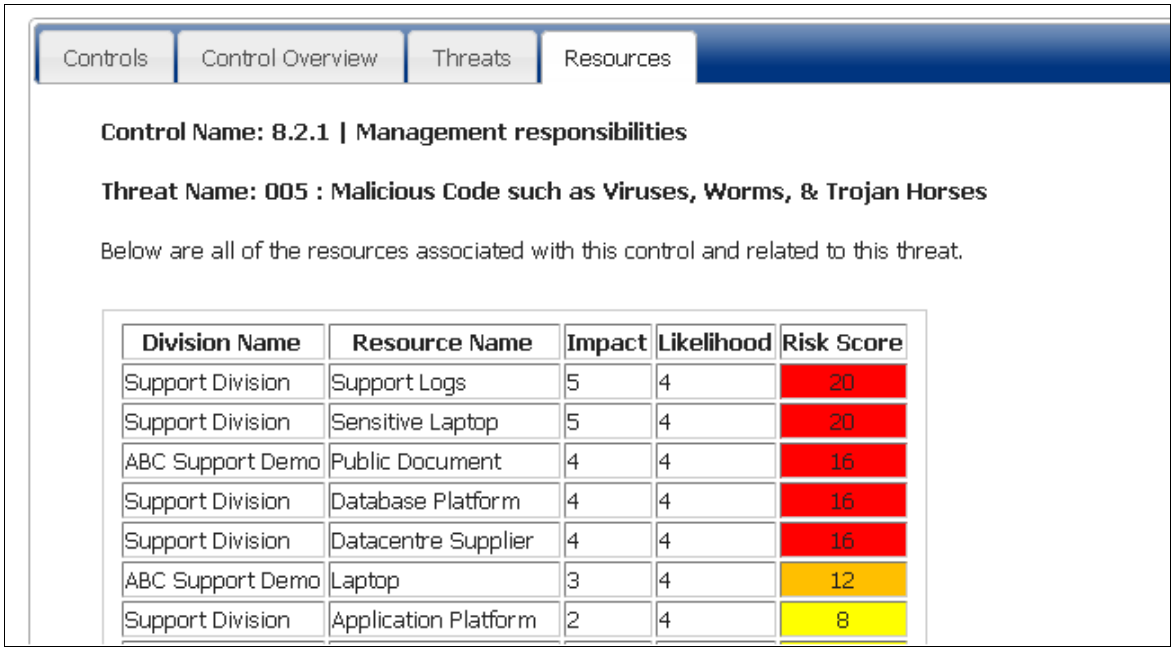


**Figure 8 - Resource Risk Score**

# Appendix A. List of figures