URM

ULTIMA RISK MANAGEMENT

ISO 27001 : 2013 Method Statement

Prepared for

Abriska 27001

1.0 Preface

1.1 Prepared By

Name	Function
Matt Thomas	Product Manager

1.2 Reviewed and Authorised By

Name	Function
Martin Jones	Managing Director

1.3 Contact Details

Address	Telephone
Ultima Place 448a Basingstoke Road Reading Berkshire RG2 0RX	0118 902 7450

1.4 Change History

Version	Date	Revision Description
1.0	July 2014	Final

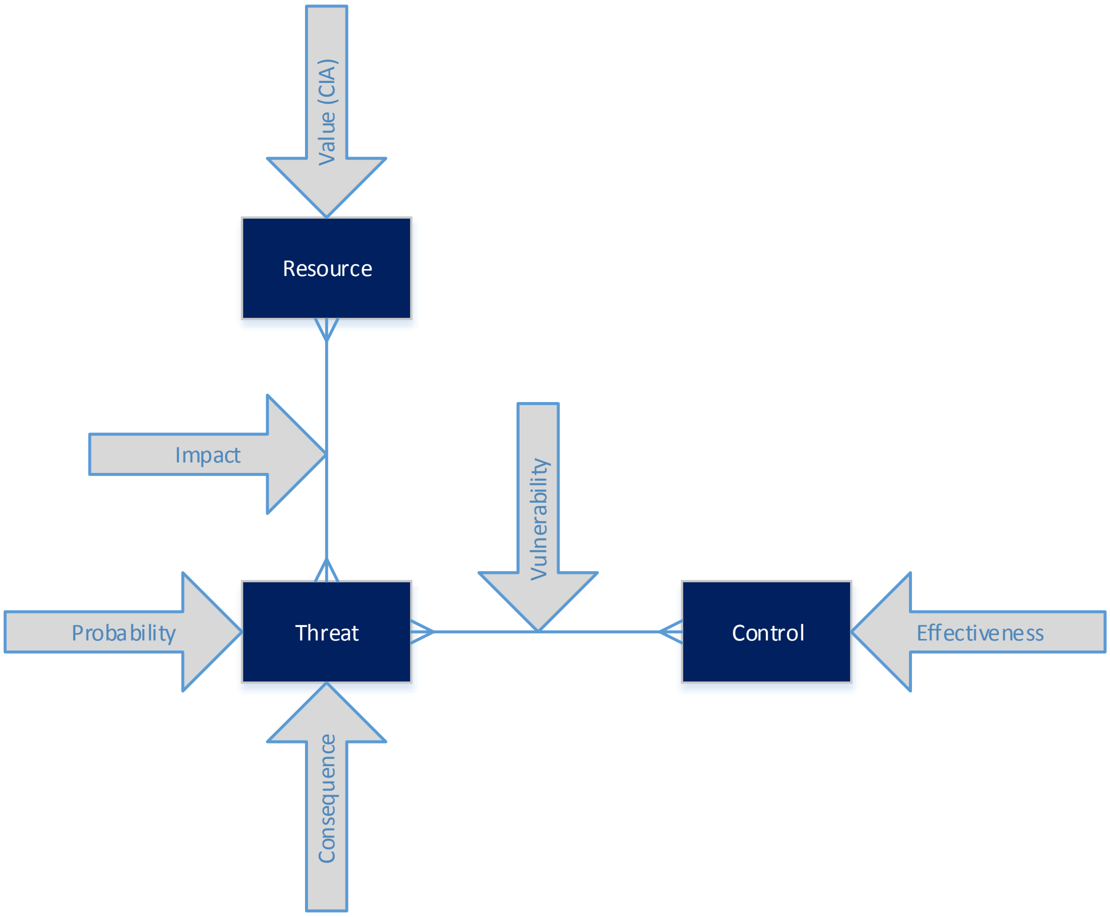
Contents

2.0 High Level Methodology

2.1 Terminology

Below is the high level methodology for completing risk assessments within Abriska for ISO 27001. All of the terminology within Abriska is customisable, therefore navigate to the methodology page within Abriska for a detailed breakdown of the methodology.

Figure 1 - High Level Methodology



Resource – Within Abriska, this is utilised to represent **Information** and **Information Process Facilities** – "*any information processing system, service or infrastructure, or the physical location housing it*"; source ISO 27000:2014

1. **Value** in terms of Confidentiality, Integrity and Availability

Threat – "*potential cause of an unwanted incident, which may result in harm to a system or organization*"; source ISO 27000:2014

1. **Probability** – each threat is assessed in terms of how likely the threat is to occur; probability is based only on factors that are outside of the organisation's control. Possible factors can include:
    - Historical security events
    - Motivation - the attractiveness of the organisation's information resources
    - Local circumstances – such as proximity to a threat source or number of users
    - Capability – the ease with which this threat can be performed
2. **Consequence** – should the threat occur there will be a loss of confidential, integrity and availability, this value is assessed for each threat

Control – "*Controls include any process, policy, device, practice, or other actions which modify risk*"; source ISO 27000:2014.

1. **Effectiveness** – this is an assessment of how well the control is implemented based on a maturity model and the guidance within ISO 27002
2. **Vulnerability** – because each threat is linked to a number of controls, based on the minimum effectiveness of these related controls a vulnerability score can be calculated.

2.2 Risk Calculation

For each resource threat combination a risk score is produced, using the following variables:

1. **Impact –** Based on the related **value** of the resource and the **consequence** of the threat a single impact score is calculated for each threat/ resource combination
2. **Likelihood** "*chance of something happening*" ISO 27000:2014 – Is a measure of how likely a threat is to occur, a combination of **probability** and **vulnerability** (i.e. both and internal factors)

Risk - equals Impact multiplied by Likelihood, the risk is then mapped onto the risk appetite to give a coloured priority. Based on the relational data above, Abriska populates the risk register with generated risk statements.

3.0 Resources, threats, controls and risks framework

3.1 Resources

Within Abriska, the term resource is used to represent the organisations information and information processing facilities (referred to as 'information assets' within ISO 27001:2005). There are standard resource types available, however these can be customised and added to within the system.

As Abriska is used for both information security and business continuity, 'Resource' was used to standardise with terminology from ISO 22301.

"All assets, people, skills, information, technology (including plant and equipment), premises, and supplies and information (whether electronic or not) that an organization has to have available to use, when needed, in order to operate and meet its objective" Source: ISO 22301:2012

3.2 Threats

Abriska bases risks on different threat types. The threats included in any risk assessment will vary according to the resource types which are subject to review. Additional threats can be added to the tool via the user interface.

3.3 Controls

The base controls framework used by Abriska is that specified in *ISO/IEC 27001: 2013 Information Technology — Security Techniques — Information Security Management Systems — Requirements* (ISO 27001) thus creating an excellent base for compliance with ISO 27002 and for use on ISO 27001 certification projects. Additional controls can be added to the tool via the user interface.

3.4 Mapping of Threats, Controls and Resources

In order for Abriska to provide risk assessment and risk management functionality, each of the resources that are added into the tool need to be mapped to each of the threats (e.g. are paper based threats affected by fire, viruses). Each of these threats are then mapped to the controls. For the base list of resource types, threats and controls this mapping is provided by default.

As a result of this mapping, any organisation adding either a new resource type, threat or control must ensure that the additional feature must be mapped (i.e. a new threat must be mapped to the appropriate control(s) or the new control mapped to the appropriate threat(s)). Failure to do this mapping will result in a loss of integrity in the risk assessment process. All of this is visible and fully customisable via the user interface.

3.5 Risk Register

Abriska generates a risk register based on these relationships between resources, threats and controls. Abriska converts this relational data into a risk statement which can be easily presented to senior management without explaining each of these concepts.

4.0 Resources

4.1 Identify Resources

All resources that need to be included in the risk assessment can easily be loaded into Abriska. The resources should be identified in terms of the characteristics of the organisation, its location, and resources and technology. Resources that are entered should be grouped according to their risk profile and value (in terms of confidentiality, integrity and availability). All resources need to be classified in terms of type, the following types are provided by default:

- Equipment
- Information - Digital
- Information - Physical
- People
- Premises
- Suppliers
- Technology

The above types are available by default; however any number of further types can be added.

Individual information resources must be separated into the above groups, for example a document management system is a piece of software with related hardware and therefore this would be represented as two resources within Abriska. Relationships between resources can be modelled within Abriska.

4.2 Identify Value of Resources - Business Impact Analysis

This phase of the risk assessment is used to assess business impacts that might result from breaches of security. The analysis considers the consequences of a loss of confidentiality (C), integrity (I) and availability (A) in business terms.

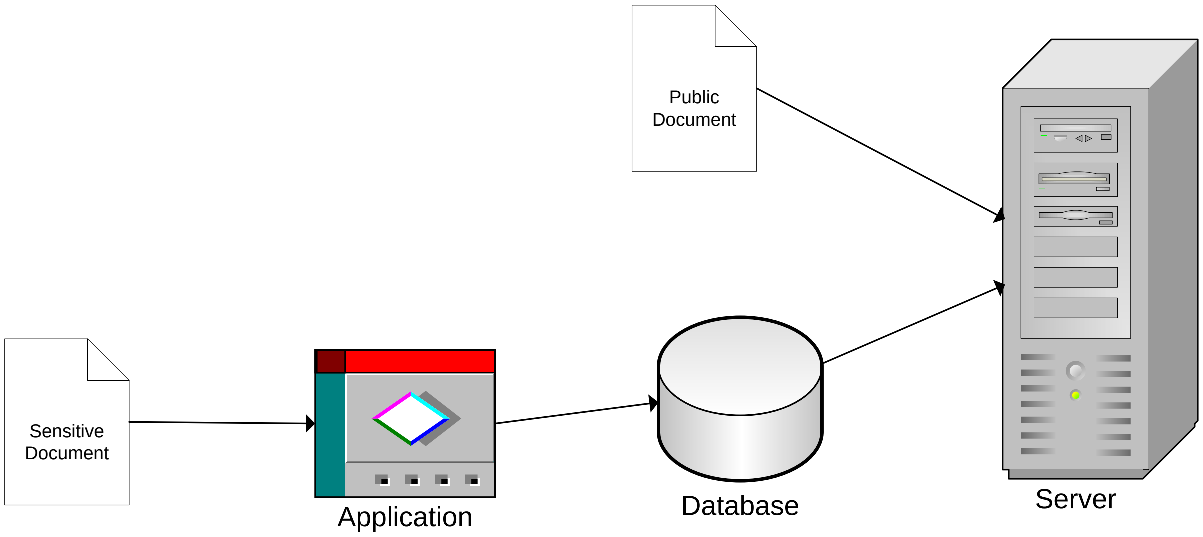
Business impacts should be quantitative as well as descriptive. For example, a loss of integrity may lead to fraud but this is relatively meaningless in business terms unless the extent of the potential for fraud is quantified. Each level of impact should be defined to provide a level of consistency. The matrix used for this business impact analysis can be see within Abriska within:

```
Organisation > Resources > Resource Attributes
```

Business impacts should be based on realistic but worst case scenarios and ignore implemented controls (since an impact is potentially the result of the failure of a control).

Business impact can be quantified against an individual resource or can be inherited from a related resource. This allows a consistent level of impact to be allocated to associated resources. For example suppose a document management system (DMS) sits on a server that also holds some public files (*Figure 2 – Resource Inheritance*). If the documents within the DMS were classified in terms of C, I and A, these values are inherited down the chain so that the application, database and server all inherit the same BIA values. The server also inherited the public documents BIA values but would use the worst case values for use within the risk assessment. At any level of the chain the inheritance can be broken for a specific attribute (C, I and A), to take account for a manual aggregation of impact values.

Figure 2 – Resource Inheritance



5.0 Threat identification

Threat – “*potential cause of an unwanted (information security) incident, which may result in harm to a system or organization*”; source ISO 27000:2014.

Abriska includes a library of threats which cover various types including technical, physical, environmental, natural disaster, people and man-made threats. These threats are linked to controls from ISO 27002 and ISO 27001 so that recommendations for controls are appropriate to identified areas of risk. This is a vital part of the risk assessment and is a major feature of Abriska since the mapping is pre-set and requires no further user intervention.

Each threat could potentially cause an impact on one or more resource types and by default is mapped to the various resource types within the default library.

5.1 Threat Impact Assessment

5.1.1 How to enter impact

Impacts result when vulnerabilities of resources allow threats to cause an unwanted incident that triggers some kind of business damage. The type of damage can vary but includes direct financial loss (e.g. from a fraud), loss of reputation (e.g. due to bad publicity) and litigation (e.g. by failing to comply with data protection or copyright legislation).

Different threats will also cause different types of security breach. For example, the threat of fire will result in loss of availability whilst unauthorised access can lead to a loss of both confidentiality and integrity. So rather than evaluate each threat/resource combination, each resource is scored in terms of the impact of a loss of C, I and A, and each threat is described in terms of how it would affect the C, I and A of the associated information. Abriska then calculates the impact to a specific resource by performing the calculation (described in Section 5.1.2 - *How* business impact is calculated).

As each resource will have been evaluated in terms of confidentiality, integrity and availability during the BIA phase (see section *4.2-Identify Value of* Resources - Business Impact Analysis), only impact distributions need to be entered against each threat. The threat impact distributions used for this threat assessment can be seen in Abriska within:

```
Organisation > RA Setup > Organisational Threats > Threat > Threat Attributes
```

or

```
Organisation > Entities > Entity > Impact & Likelihood > Threat
```

5.1.2 How business impact is calculated

Abriska considers each threat to result in 100% impact but that this is distributed across the different facets of information security (i.e. C, I and A) as they relate to a specific threat. For example, the threat of fire will cause 100% loss of availability as there will be no direct impact relating to confidentiality or integrity.

The following examples illustrate how this is calculated.

Business impacts against the specific resource, as assessed by the information owner, are as follows:

• Loss of confidentiality:	3 out of 5
• Loss of Integrity:	2 out of 5
• Loss of availability:	3 out of 5

Table 1 shows how the threat (Malicious Code) might impact in terms of C, I and A.

Table 1 - Malicious Code

Threat Name	C	I	A	Impact
1) Malicious Code such as Viruses, Worms, & Trojan Horses	10%	75%	15%	
2) Resource Impact scores	3	2	3	
3) Calculation	10% x 3 =	75% x 2 =	15% x 3 =	
Impact contributions	0.3	1.5	0.45	2.25

In the above example, it has been assessed that manifestation of the threat will result in a 10% loss of confidentiality, 75% loss of integrity and 15% loss of availability (as shown in row 1). Given the assessed Resource Impact Scores (as shown in row 2), the table then shows (as shown in row 3) how the final impact for this threat/resource combination is calculated as 2.25.

Table 2 - Operations Error

Threat Name	C	I	A	Impact
1) Operations Error	0%	25%	75%	
2) Resource Impact scores	3	2	3	
3) Calculation	0% x 3 =	25% x 2 =	75% x 3 =	
Impact contributions	0	0.5	2.25	2.75

Table 2 shows how the threat (Operations Error) might impact the same resource in terms of confidentiality, integrity and availability. The same calculations apply as Table 1.

5.2 Threat Probability Assessment

A number of factors are used to assess the probability of a threat occurring that lead to an increase in the probability of an impact occurring. Such factors will include:

- The attractiveness of an information resource
- Historical security events
- Local circumstances
- Number of users
- Attitude of management.

Probability is assessed for each threat against groups of resources. To enforce a level of consistency a matrix is defined that describes the different levels. Abriska can be customised to use any number of levels e.g. 1-4, 1-6. The scale must be in ascending order, the higher the number the more likely it is to happen.

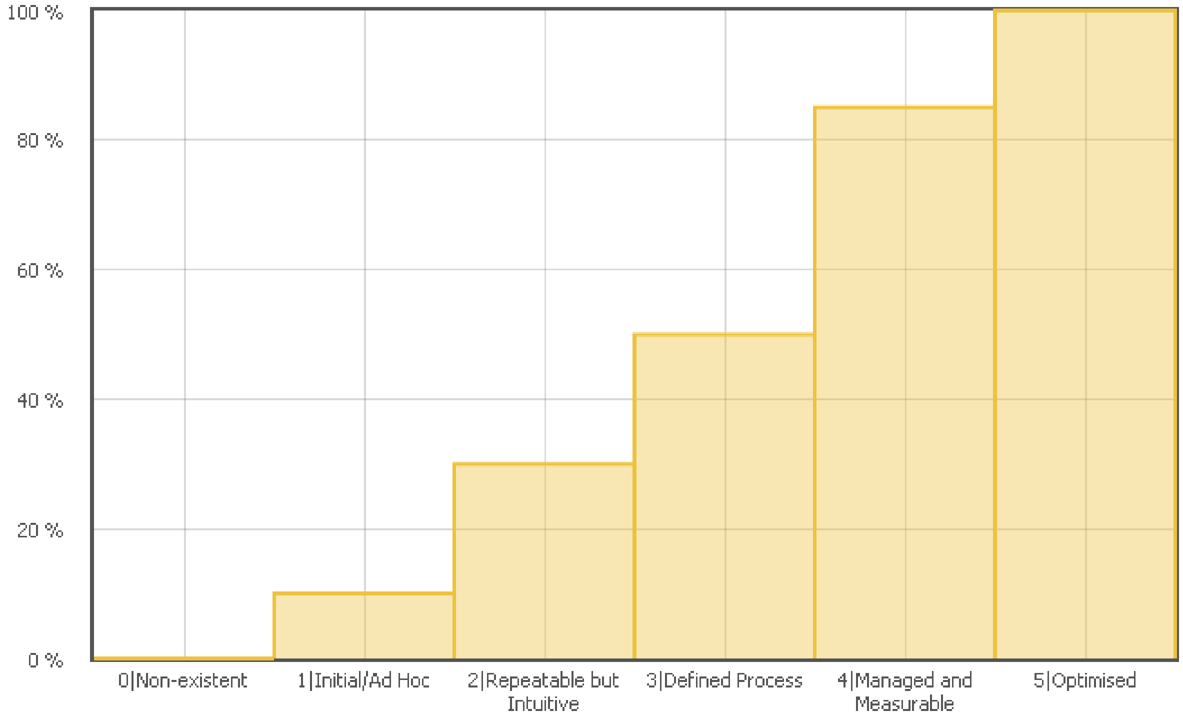
5.3 Threat Vulnerability Assessment

Vulnerability calculations are based on the maturity of the controls that are attached to those threats. Each of the controls in Abriska is rated on the same maturity model (see Section 6.0 Control Maturity Assessment for further details). Based on the maturity of the related controls each threat will have a calculated vulnerability level. If the related controls are mature, then the vulnerability of the information resource to that threat will be lower.

It is important to consider that the relationship between control maturity and vulnerability is not linear (i.e. there may be different levels of vulnerability improvement between different control maturity levels.). This is due to the fact that the effectiveness of the control would vary across the different levels of maturity.

For example, a control would be considered 0% effective if it is non-existent and 100% effective if it is at maximum maturity (optimised). But if a control was “Managed and Measurable”, it might be determined that it’s 85% effective. This non-linear effectiveness can be explained by the diminishing returns received by implementing a control to the highest maturity level. At the other end of the maturity scale, a control that is perform on an ad hoc basis is only partially effective so therefore doesn’t provide much of a reduction in vulnerability. A breakdown of the control effectiveness is detailed in *Figure 3 - Control Effectiveness.*

Figure 3 - Control Effectiveness



This figure is used to modify the vulnerability value, and when combined with the value that has been assessed for probability, gives a level of likelihood for the threat to occur.

6.0 Control Maturity Assessment

Each control that is defined within Abriska needs to be assessed to understand how the control has been implemented and any vulnerability that might be introduced to the environment as a result of this control's implementation.

To ensure that a consistent approach is applied to this assessment a maturity model is used throughout the control assessment. The maturity model used for this control maturity assessment can be seen in Abriska within:

```
Organisation > CMA Setup > Maturity Model
```

As different areas of the organisation may have implemented controls to a different maturity Abriska allows controls to be assess at any level of an organisation's hierarchy. For example, control 12.1.1: Documented operating procedures, will be implemented throughout the organisation but may differ in terms maturity level.

This is an important concept, as control maturity should be directly proportional to the information resources value. For example, suppose an organisation exists with the following structure:

- ABC Design Firm
  - Sales
  - Design Team
  - IT

All divisions own information resources. The design team's information resources (intellectual property for example) are highly confidential to the organisation, therefore controls that protect the confidentiality of their resources are paramount.

The sales team does not own such confidential resources therefore based on the organisation's risk appetite the control around the confidentiality of its resources could be weaker.

The IT team looks after the servers that contain the information of both departments (see section *4.2 - Identify Value of* Resources - Business Impact Analysis for a detail of this inheritance), therefore its controls will also need to be strong.

Ultimately this control maturity affects the likelihood of a threat occurring, if the control is mature then the threat is less likely to occur. If the control is non-existent or weak then this will do nothing to reduce the likelihood of this threat. This calculation is detailed in section *5.3-Threat Vulnerability Assessment.*

Whilst assessing the controls, recommendations for improvement are provided as appropriate, along with the expected maturity of the control should the recommendation be implemented. This allows a projected risk score to be calculated.

During the assessment, any specific vulnerabilities should be raised within specific vulnerabilities section (see section 8.0 Specific Vulnerabilities).

7.0 Risk Calculation

7.1 Risk Calculation

Abriska calculates three levels of risk, each of which are described below:

1. **Absolute Risk** – this represent the risk of a particular threat occurring excluding the influence of current controls. From the risk variables described above, this is calculated as *Impact x Likelihood not taking into account current controls.*
2. **Current/Controlled Risk** – this represents the current risk score. It is based on the absolute risk with the current control effectiveness taken into account. From the risk variables described above this is calculated as *Impact x Likelihood taking into account Current Control Effectiveness.*
3. **Residual/Treated Risk –**this represent the proposed risk score should the recommendation be implemented. It is based on the absolute risk with the proposed control effectiveness taken into account. From the risk variables described above this is calculated as *Impact x Likelihood taking into account Proposed Control Effectiveness.*

The names associated with each level can be modified within the risk assessment setup of Abriska. As there are specific elements within the organisation that can be configured separately the specific methodology for an organisation can be viewed within the organisation:

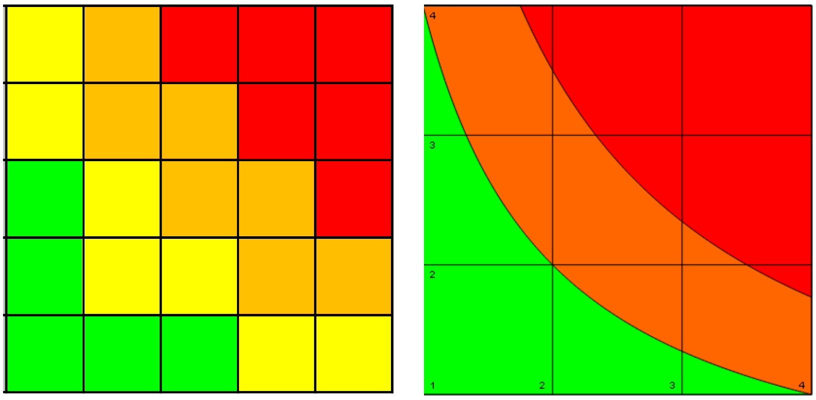
```
Organisation > RA Setup > ‘Methodology’ tab
```

7.2 Risk Appetite

The risk appetite within Abriska is represented by the using a matrix of likelihood and impact. The risk appetite matrix used for within Abriska can be viewed within:

```
Organisation > RA Setup > Risk Appetite
```

Figure 4 - Risk Matrix



7.3 Example Risk Calculation

7.3.1 Example Configuration

As an example of how Abriska calculates each level of risk, suppose Abriska was configured with a single threat, resource and control. All scores are out of 5, with 5 being high.

7.3.1.1 Resource

	Confidentiality	Integrity	Availability
Resource Impact Scores	4	4	4

7.3.1.2 Threat

	Confidentiality	Integrity	Availability
Threat Consequence Scores	4	4	4

Threat Probability Score: 5

7.3.1.3 Control

Current Control Maturity: 1|Initial/Ad Hoc

Proposed Control Maturity: 5|Optimised

7.3.2 Resource Risk Score

The resource will have three levels of risk associated with each applicable threat:

Absolute Risk

Impact [4] X Likelihood [5] (Probability [5] and Vulnerability [5] i.e. the maximum it can be)

The level of risk is equal to 4 x 5 which gives a risk score of 20.

Current/Controlled Risk

Impact [4] X Likelihood [4.6] (Probability [5] and Vulnerability [4.6] i.e. lookup '1|Initial/Ad Hoc' within Figure 4 - Example Likelihood Scale)

The level of risk is equal to 4.6 x 4 which gives a risk score of 18.4

Residual/Treated Risk

Impact [4] X Likelihood [1] (Probability [5] and Vulnerability [1] i.e. lookup '5|Optimised' within Figure 4 - Example Likelihood Scale = 1)

The level of risk is equal to 1 x 4 which gives a risk score of 4

7.3.3 Control Risk Score

The table below (Figure 5 - Risk Calculation Control Example) shows a control from the risk treatment plan. Using the values above the control calculates the level of risk associated with each of the threats that it is related to.

As more threats are added and linked to each threat the risk score will be the highest related risk associated with this control. For each control that is implemented throughout the organisation, a risk treatment plan will be produced. This will allow an assessment to be made as to the suitability of the current control implementation. This is assessed based on the risk score of the attached threats.

Figure 5- Example Likelihood Scale

From the table below the tan colours show how the likelihood value is calculated based on the probability and vulnerability score.

			Probability				
Minimum Related Maturity Level	Maturity Effectiveness Level	Vulnerability Score	5	4	3	2	1
0|Non-existent	0%	5	5	4	3	2	1
1|Initial/Ad Hoc	10%	4.6	4.6	3.7	2.8	1.9	1
2|Repeatable but Intuitive	30%	3.8	3.8	3.1	2.4	1.7	1
3|Defined Process	50%	3	3	2.5	2	1.5	1
4|Managed and Measurable	85%	1.6	1.6	1.45	1.3	1.15	1
5|Optimised	100%	1	1	1	1	1	1

Figure 6 - Risk Calculation Control Example

Control Ref	Control Name	Current Implementation	Current Maturity	Absolute Risk Score	Controlled Risk Score	Recommendation	Recommendation Maturity	Residual Risk Score
8.2.2	Information security awareness, education & training	All staff attend an awareness session at induction time, however no on-going training is conducted at regular intervals.	1:Initial/Ad Hoc	20	18.4	Provide additional training, including additional awareness materials such as newsletters and a quiz.	5:Optimised	4

8.0 Specific Vulnerabilities

Abriska allows specific vulnerabilities to be raised to customise each risk variable which is calculated or entered into Abriska. For example, support that one system within the organisation operates on legacy hardware, rather than lowing the control maturity associated with a control across the organisation, a specific vulnerability can be raised which overwrites the calculated value for a specific resource - threat combination.

A library of example vulnerabilities is available within Abriska within:

```
Organisation > Entities > Entity > Identify Vulnerabilities
```

Each vulnerability can overwrite the value for vulnerability, probability or impact for any specific resource threat combination.

The risk associated with each vulnerability will be calculated and the maximum risk score will be reported to the user to allow a risk treatment decision to be made.

9.0 Risks Statements

Abriska generates a list of risk statements which express the top risks to the organisation. Each risk statement is generated in a generic format which can then be overwritten by the user. The following format is utilised:

Threat to **Supporting Resource| Information Processing Facilities** will affect the {C, I and A} of **Information** due to {maturity of Control(s)| Vulnerability}.

E.g.

A. Power failure to email system will affect the Availability of Customer Data due to a lack of 11.2.2 Supporting Utilities.
B. Theft by third parties to Reading Office will affect the Confidentiality of Client Folders due to a lack of 11.1.6 Delivery and loading areas.
C. Technical Failure of a Main Computer or its Storage Devices to AS400 will affect the Integrity and Availability of Client Data due to Legacy Hardware.

Each risk statement can be overwritten to provide a clearer statement, for example, Statement B above could be re-written as "*Theft of client folders from the warehouse by delivery drivers due to insufficient segregation between incoming and outgoing post*"

Each risk statement has a risk score associated with it and is available within the online risk register. The ability to assign a risk owner and risk treatment decision is available from this page.

Output:

Risk Register – outputs each of the risk statements, the risk treatment decision and the owner. Each risk that is identified should be reviewed and undergo treatment by applying one of the following:

- Reduce – Apply the recommendation and improve the appropriate control
- Accept – Knowingly and objectively accept the risk
- Avoid – Change the business or environment to stop completing the related activity
- Transfer – Outsource/transfer the risks to other parties.

NB: the standard risk treatment decisions can be customised by the organisation.