1.0 Introduction

Abriska has been (re)designed to produce a risk assessment in line with the methodology encapsulated within ISO 27001:2013, the latest version of the International Standard for Information Security Management. The objective of this document is to clarify how Abriska completes a risk assessment and how it satisfies the requirements of ISO 27001:2013, whilst not necessarily performing the actions in the same order as laid out in the Standard. Section 2 of this document explains how an ISO 27001:2013 compliant risk assessment can be delivered using Abriska. Section 3 of this document explains how each of the requirements within ISO 27001:2013 are satisfied by Abriska.

2.0 Abriska ISO 27001:2013 High Level Methodology

2.1 Identify Information and Supporting Assets

2.1.1 Setup

Upon creation of a new organisation, Abriska will contain the default resource types suggested by the Standard. There is no longer a requirement to identify risks to all assets, only risks to information. However, to fully understand the risks, the supporting assets that store or process the information must be identified. Supporting assets can be recorded at a high level and only those which are directly involved with information are required e.g. the documenting of supporting utilities, generators, UPS' etc. is not required. There are default resource types included within Abriska, which can be amended or added to[1].

To consistently assess the assets, an impact scale should be established and entered into Abriska to support the assessment of the Confidentiality, Integrity and Availability (CIA) of information and related information processing assets.

Risk acceptance criteria should also be established within the organisation which is represented by either an impact/likelihood matrix or based on the resulting risk score. This should be setup at the start, but can be modified throughout the assessment.

Inputs:

- Impact scales to use for assessment of Confidentiality, Integrity and Availability (CIA)
- Additional specific resource types for the organisation
- Risk appetite
    - Impact/likelihood matrix *or*
    - Risk score scale values e.g. greater than 16 equals high/ "red".

2.1.2 Operation

Information needs to be identified within the organisation. Information should be grouped at the highest possible level e.g. information types rather than specific items. Information is still valued in terms of CIA against the organisation's predefined impact scale.

Information can then be directly linked to supporting assets, which enforces a level of consistency within the asset valuation. Linkage should be minimised with links established directly between information and supporting processing assets. The objective is to ensure that all information and supporting assets are valued: the objective is not to try and create a model of all the information interactions which exist within the organisation.

Output:

- An information and supporting asset register, with all assets valued for CIA impact.

2.2 Identify and Evaluate Controls

2.2.1 Setup

A standard control library consisting of 114 controls from ISO 27002:2013 (Code of Practice) is included within Abriska, which can be added to or amended based on the organisation's requirements[1].

Inputs:

- Specific additional controls relevant to the organisation.

2.2.2 Operation

For all of the controls detailed in ISO 27002:2013, organisations will need to decide if any of these are not applicable to its operational activity. This must be justified as the control will not be excluded from any subsequent risk assessment activities. The default controls documented in ISO 27002:2013, and included in Abriska, should be expanded to include any additional legal, regulatory or contractual controls applicable to the organisation[1].

For each applicable control, organisations will need to assess the current control implementation and maturity. Organisations can also define a proposed 'control improvement' recommendation and the estimated/proposed maturity associated with that improvement. Supporting documents relating to a control can be linked via an HTML link.

Output:

- Statement of applicability (SoA) which details each of the controls indicating if they are applicable along with reasons for inclusion or exclusion
- Control maturity report highlighting current and proposed control maturity.

2.3 Identify Threats and Specific Vulnerabilities to Information and Supporting Assets

2.3.1 Setup

A standard threat library is included within Abriska, which can be added to or amended based on the organisation's context/requirements.[1]

Each of the 'library' threats are related to relevant resource types (e.g. power failure affects technology) and also to the appropriate ISO 27001 control(s) which will mitigate this threat. Organisations should review Abriska's default threat linking to ensure it reflects the context of its operational activity and the types of resources it is looking to safeguard (e.g. threats and controls relevant to equipment in an office environment may be different to an industrial organisation).

Inputs:

- Specific threats to organisation.

2.3.2 Operation

An entity is created for each risk assessment that needs to be performed. An entity represents a collection of resources which face a common set of threats. Examples of entities include the whole organisation, specific locations (e.g. Bristol, Truro and London), types of site (e.g. offices, datacentres), or individual processes (e.g. finance, sales).

Having identified the resources that are to be included in a specific risk assessment activity, Abriska will bring forward a list of relevant threats (determined by the resource / asset linking). The consequence of each threat occurring is expressed in terms of CIA (% value), a URM default is

[1] All additional controls and threats will need to be appropriately linked to threats and controls respectively. Also, both threats and controls will need to be linked through to resources.

provided but must be reviewed to check on the relevance/appropriateness to each organisation. This consequence value is combined with the asset value to provide a score for impact.

The probability of each threat occurring should be reviewed and evaluated. Threat probability is evaluated without considering current controls and should be based on a realistic worst case scenario for all of the information within scope.

If a particular resource has a much higher probability than the other resources (e.g. laptops are more likely to be stolen) then a specific vulnerability should be raised. Vulnerabilities should be identified and related to

- Either to an information or a supporting processing asset
- One or more threat

The effect the vulnerability has on a threat should also be recorded (e.g. a laptop is taken offsite so there is an increase probability that it will be stolen).

Abriska will combine the probability value with the calculated vulnerability score (derived from control maturity see 2.2 Identify and Evaluate Controls) to produce a likelihood value.

Risk is calculated as impact x likelihood. All risks can then be compared to the risk appetite criteria established at the outset of this process. Risk can be reviewed in the following ways:

1. The risk of each threat occurring against a specific information or supporting asset
2. The risk associated with having a specific vulnerability within the organisation. This is calculated based on the related threat
3. The risk associated with having each control at the given level of maturity is calculated based on each of the threats that a given control is linked through to.

Output:

- Risk score matrix (RSM) identifying the risk of each threat occurring against each information asset and supporting asset
- A vulnerability report highlighting the associated risk of this particular vulnerability
- A risk treatment plan (RTP) which highlights the risk associated with having each control at the defined level of maturity.

2.4 Risk Statements

2.4.1 Setup

Once assets, threats and controls have each been established a risk register will be available.

2.4.2 Operation

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

Threat to **Supporting Asset** will affect the {C, I and A} of **Information Asset** due to a {Lack 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 Head 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 will have a risk score associated with it and will documented within the online risk register. The ability to assign a risk owner and risk treatment decision is also available.

Output:

- Risk Register – outputs each of the risk statements, the risk treatment decision and the owner.

3.0 ISO 27001:2013 Risk Assessment Requirements

ISO 27001:2013 Requirement	How Abriska satisfies this requirement?
6.1 Actions to address risks and opportunities 6.1.1 General	
When planning for the information security management system, the organization shall consider the issues referred to in 4.1 and the requirements referred to in 4.2 and determine the risks and opportunities that need to be addressed to: a) ensure the information security management system can achieve its intended outcome(s); b) prevent, or reduce, undesired effects; and c) achieve continual improvement. The organization shall plan: d) actions to address these risks and opportunities; and e) how to: 1) integrate and implement the actions into its information security management system processes; and 2) evaluate the effectiveness of these actions.	An organisation must define its context (4.1) and its interested parties (4.2). This information should be documented outside of Abriska usually within a scoping document. Based on the scope of the ISMS additional threats, controls or resources types may need to be added into the organisation. The intended outcomes of the ISMS are documented and the risk assessment will support this e.g. if the desired outcome is to minimise the risk of a customer information breach, then threats should be added that relate to the storage and processing of customer information . Actions are identified based on control improvements and vulnerability mitigation, but may also come from audit activity or incidents.
6.1.2 Information security risk assessment	

ISO 27001:2013 Requirement	How Abriska satisfies this requirement?
The organization shall define and apply an information security risk assessment process that: a) establishes and maintains information security risk criteria that include: 1) the risk acceptance criteria; and 2) criteria for performing information security risk assessments; b) ensures that repeated information security risk assessments produce consistent, valid and comparable results;	Abriska method statement describes its operation, calculation criteria and describes how repeatable results are achieved. Risk acceptance criteria is defined within the appetite, the appetite levels should be related to the organisation in order to define who can accept risks at each level e.g. high/ "red" risk must be signed off by a director.
c) identifies the information security risks: 1) apply the information security risk assessment process to identify risks associated with the loss of confidentiality, integrity and availability for information within the scope of the information security management system; and 2) identify the risk owners;	Abriska allows information assets to be identified and assessed for losses in terms of CIA. To understand the risks associated with each information assets, supporting assets are identified and linked to the information assets. All information assets and supporting assets are related to a set of threats based on the asset type. Threats can be fully expressed with either a related vulnerability or control to express a risk statement. All risk statements have an owner.
d) analyses the information security risks: 1) assess the potential consequences that would result if the risks identified in 6.1.2 c) 1) were to materialize; 2) assess the realistic likelihood of the occurrence of the risks identified in 6.1.2 c) 1); and	Each risk is assessed in terms of consequence and likelihood. Likelihood is calculated based on the users assessment of probability combined with the assessment of current control maturity.

ISO 27001:2013 Requirement	How Abriska satisfies this requirement?
3) determine the levels of risk; e) evaluates the information security risks: 1) compare the results of risk analysis with the risk criteria established in 6.1.2 a); and 2) prioritize the analysed risks for risk treatment. The organization shall retain documented information about the information security risk assessment process.	Risk is calculated as impact multiplied by likelihood and is compared against the risk appetite. Risk can be shown in a variety of ways: • Risk of threat occurring against a specific resource • Risk of control at current level of maturity • Risk of vulnerability affecting a specific resource • Fully expressed risk statements
6.1.3 Information security risk treatment	
The organization shall define and apply an information security risk treatment process to: a) select appropriate information security risk treatment options, taking account of the risk assessment results; b) determine all controls that are necessary to implement the information security risk treatment option(s) chosen; NOTE Organizations can design controls as required, or identify them from any source.	Each risk statement has a risk strategy associated with it.
c) compare the controls determined in 6.1.3 b) above with those in Annex A and verify that no necessary controls have been omitted; NOTE 1 Annex A contains a comprehensive list of control objectives and controls. Users of this International Standard are directed to Annex A to ensure that no necessary controls are overlooked. NOTE 2 Control objectives are implicitly included in the controls chosen. The control objectives and controls listed in Annex A are not exhaustive and additional control objectives and controls may be needed.	All ISO 27001 Annex A controls are included within Abriska by default. Should an organisation wish to add any extra controls, they can be added through the interface.

ISO 27001:2013 Requirement	How Abriska satisfies this requirement?
d) produce a Statement of Applicability that contains the necessary controls (see 6.1.3 b) and c)) and justification for inclusions, whether they are implemented or not, and the justification for exclusions of controls from Annex A;	Abriska produces a SoA for all controls within the organisation (at least the 114 contained within ISO 27002:2013). Each control can be justified for inclusion or is justified by default as relating to specific threats. An implementation status can be recorded and if a control is excluded a free text justification must be entered.
e) formulate an information security risk treatment plan; and	A RTP is produced which details all of the controls that require improving. A Vulnerability Treatment Plan is also produced which includes the addressing of specific vulnerabilities.
f) obtain risk owners' approval of the information security risk treatment plan and acceptance of the residual information security risks. The organization shall retain documented information about the information security risk treatment process.	The Risk Register details the residual risk associated with each risk statement and should be formally accepted during an *information security management meeting*.