1.0 Abriska migration from ISO 27001:2005 to ISO 27001:2013

Further to the release of ISO 27001:2013, the purpose of this update is to outline the Abriska migration plan from ISO 27001:2005 to ISO 27001:2013.

1.1 Methodology

The Abriska methodology remains compliant with the requirements of ISO 27001:2013. The new version is less prescriptive in its approach with reference to the ISO 31000 risk assessment requirements i.e. no explicit reference to threats and vulnerabilities but refers to causes and sources of risk instead. However, in the introduction section of ISO 27002:2013, 0.2 Information security requirements, it states that:

Through a risk assessment, threats to assets are identified, vulnerability to and likelihood of occurrence is evaluated and potential impact is estimated

URM's recommendation is that threats and vulnerabilities are still considered during the risk assessment in order to provide the appropriate level of granularity.

1.2 Changes to Abriska

1.2.1 Controls

The controls within ISO 27001:2013 have been updated. The new version contains 114 controls in Annex A as opposed to 133 in the 2005 version. The controls are now are listed under 14 security clause headings and 35 security categories, rather than 11 security clause headings and 39 security categories in the previous version.

Some controls have been deleted as they are no longer considered commonplace in an interconnected world, whilst others have been merged together as they were really only different ways of saying the same thing. There are some new controls, which even though not necessarily new in concept have been given more prominence by being separated out in the new Standard.

As part of the risk treatment process, organisations should 'determine all controls that are necessary…' and then compare this list with the controls in Annex A to 'verify that no necessary controls have been omitted'. A note to the risk treatment clause (6.1.3) states that 'Organisations can design controls as required, or identify them from any source'. URM has mapped the 2005 controls with the 2013 controls identifying those that are new, those that have been deleted and those that have been merged, clarified, extended or replaced. URM has also considered additional controls that organisations may wish to also consider.

1.2.2 New Workflow and Reports

The new Standard requires risk owners to be identified and for them to accept the proposed risk treatment plan (RTP) and any residual risks. It is understood that a risk owner could be an asset/resource owner, control owner or someone else (such as a business unit owner). Therefore, a risk register has been added into Abriska, which is an auto-generated list of risk statements which can be allocated to individuals or teams including risk score values and risk decisions.

New reports will also be added to allow this risk register to be exported from Abriska.

1.3 Timeline for Proposed Changes

URM has enhanced Abriska to reflect the changes in ISO 27001:2013 to ensure that the tool remains compliant with the Standard. This version will be released into the main live environment in November 2013, however each organisation will have the option of when to migrate to the new version. As the certification bodies (CBs) are not yet able to assess the requirements of the new Standard[1], if an organisation transitions to the new Standard there is a risk that a non conformity could be raised during a continuing assessment visit (CAV) i.e. for an incorrect Statement of Applicability. It is likely that the certification bodies will be accredited to deliver ISO 27001:2013 certification in the first half of 2014.

When the CBs confirm that they are able to assess to the new Standard, each client will be able to transition to the new version of Abriska. URM will also deliver a series of transition workshops, free of charge, at its Reading premises, addressing how to migrate from the current version of Abriska to the new version. This will include a high level discussion on the control mapping.

URM will provide the following migration options with regard to the version of Abriska:

1. **'Reset'** – this will involve deleting all control maturity assessments, adding the new controls and new threat mapping. Each client will then be responsible for undertaking a control maturity assessment of all of the new controls
2. **'Migrate'** – All old controls will be archived and the facility to review the archived controls will be made available (including maturity assessments). The new controls will be added and based on URM's mapping of 2005 – 2013 controls, a maturity value and implementation description for the new controls will be defaulted. Where a new control has replaced a number of old controls, the new control will inherit the lowest control maturity value of the previous controls. Each client will be responsible for reviewing and verifying the migrated maturity assessments and evaluating any new controls
3. **'Bespoke'** – Any specific organisation requirements can be discussed including quoting for additional support.

Further information will be made available when the CBs confirm when they are able to transition their clients.

[1] URM is liaising with the CBs and understands that transition will be assessed during a CAV and that CBs are NOT allowed by the UK Accreditation Service (UKAS) or ANSI-ASQ National Accreditation Board (ANAB) to issue unauthorised certificates. Therefore until the CBs are accredited by UKAS/ANAB, they will continue to offer certification to ISO 27001:2005.