URM

Getting the balance right

Abriska 27036

Supplier Risk Management Tool

Focusing on information and cyber security, Abriska 27036 is designed to assist you assess and minimise your supply chain risks.

www.urmconsulting.com

Business Challenge

In order to achieve business goals, nearly all organisations are dependent on third parties for support. Some of these suppliers may have access to some of your very sensitive information, or perhaps access to your network, whilst others may be providing a critical activity which your organisation relies upon to deliver its key products and services. The challenge is assessing the risks associated with a large number of diverse suppliers and third parties and understanding whether the information security measures they have in place are in line with their expectations/controls. Often, a single questionnaire, 'one size fits all' is sent to all suppliers, irrespective of how critical that supplier is. By utilising a single, common questionnaire, it is almost impossible to ensure that it is sufficiently detailed or searching for critical suppliers. Conversely, the single questionnaire approach may be too detailed and inappropriate for low risk suppliers.

Once sent, the next issue for many organisations is managing the questionnaire responses and analysis. This is typically dependant on manual processes to both chase suppliers to complete the questionnaire and then analyse the completed forms. Abriska 27036 has been developed specifically to address the challenge of conducting tailored supplier information security risk assessments and meeting the requirements of ISO 27036, the International Standard information security for supplier relationships. This Abriska module can be deployed independently or as part of a wider Abriska implementation.

Figure 1 – Supplier Risk Management Methodology

Supplier Risk Management Methodology

With Abriska 27036, you are able to create and send tailored questionnaires to any supplier or third party. The complexity of questionnaires can be varied according to the type and the status of supplier and the dynamic workflow within the questions allows additional detailed questions to be asked where necessary. The questions can be chosen from the extensive bank within Abriska 27036 or designed specifically.

The supplier contact will receive an email notification to log on to the system to complete the questionnaire online. The supplier is able to upload evidence in the form of documents or links to files to support their responses. Once the questionnaire has been completed, a notification is received and the detailed questionnaire responses can be reviewed and analysed. Abriska completes an initial triage of the response by comparing the supplier's answers against your organisation's risk appetite and assigns the supplier a risk score.. This helps you to assess the risk that the supplier poses and to then interrogate the detailed answers and supporting evidence.

Following the risk assessment, risk treatment can be conducted and actions allocated either to the supplier or to individuals within your organisation. Abriska 27036 comes preloaded with a list of questions and typical supplier categories, however these questions can be tailored by you or specifically for an individual supplier.

Abriska 27036: Step by Step

Categorisation of Suppliers

Abriska contains a supplier register which allows all suppliers to be loaded into the system and assigned both an internal owner and a supplier contact. Abriska is pre-configured with detailed supplier categories (e.g. cloud service provider, accesses the corporate network, stores personal data) which are mapped to controls from best practice standards. Additional categories can be easily created by the organisation e.g. accesses patient identifiable data and suppliers can be assigned to one or more categories.

Prioritisation of Suppliers

For information security assessments, each supplier is prioritised by the information that they have access to e.g. an outsourced HR provider would be prioritised based on the sensitivity of personal/ HR data which they can access. This is achieved by either assessing the confidentiality, integrity or availability of information the supplier can access or by linking an information type through to the supplier e.g. HR information > outsourced HR provider. This step ensures that questionnaires, and ultimately, the required controls you expects a supplier to implement, are appropriate to the information being stored, processed or transmitted.

Supplier Assessment

Once a customisable email has been sent, the supplier logs onto Abriska, creates a profile and is able to access the questionnaire which you have configured for them. The supplier answers the questions online and all answers are saved directly into Abriska. Each questionnaire is specific to the supplier based on the categorisation that has been completed and branching of questions is possible to ensure that more detail is obtained where appropriate e.g. if a supplier confirms it outsources software development, it will be required to answer further questions about controls in place.

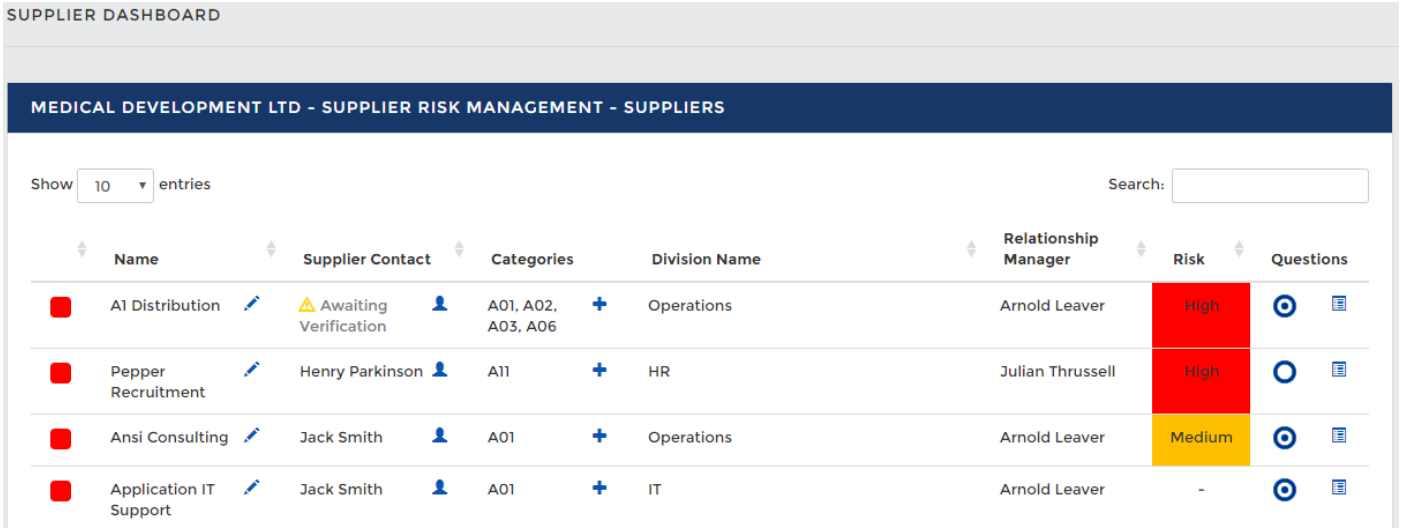

Figure 2 – Supplier Risk Dashboard

Reporting, Risk Treatment and Actions

Once the questionnaire has been completed, you are notified and are able to analyse the questionnaire responses. The supplier is assigned a risk rating based on their answers and the assigned priority. This score is colour coded according to your pre-defined risk appetite e.g. a red, amber or green rating. A risk treatment decision (e.g. whether to reduce, accept, avoid or transfer the risk) is then recorded and appropriate actions can then be entered into the system. These actions can either be allocated to the supplier or to an individual within your organisation. The questionnaire process can then be repeated at a time interval appropriate to the supplier.

How Abriska 27036 Can Benefit Your Organisation

Robust

Typically, organisations use email and attachments to send and receive questionnaires with third parties. Often, the same questionnaire is sent to all suppliers regardless of the services they provide. Abriska 27036 allows each supplier to be categorised, according to the services they provide and then for tailored questionnaires to be sent and completed via a secure online portal. All responses are maintained so that improvements over time can be demonstrated.

Flexible

Abriska 27036 has been designed to allow an organisation to customise the questionnaires, categorisations and associated methodology directly through the interface. The system comes pre-configured with defaults e.g. supplier categories, questions and workflow; all this can be tailored to your specific requirements or to a totally bespoke methodology.

Cost and Time Saving

Abriska 27036 eliminates the manual administration involved in sending and managing the questionnaire response, e.g. Abriska can be configured to send reminder emails to suppliers who have not completed a questionnaire or when a questionnaire is due for review. Abriska 27036 also facilitates time saving by completing an initial triage of the response by comparing the supplier's answers against your organisation's risk appetite and assigns the supplier a risk score.

Distribution of Responsibility

Being an accessible, web-based application, Abriska 27036 enables multiple users to work on supplier assessments together, regardless of location, thus simplifying the collaboration process. With each supplier directly accessing Abriska, there is no need to spend time amalgamating the suppliers' responses into a central repository.

Pre-configured

URM's consultants have developed a standard set of questions enabling your organisations to quickly start the process of conducting third party risk assessments without lengthy configuration. The questionnaire can be easily updated with additional questions. URM can import these questions or you the organisation can create bespoke questions through the interface.

Integration

Abriska 27036 is integrated with the other Abriska modules, providing a holistic view of risk management and audit activities. Supplier risks will be treated in the same way as other risks that are raised within the organisation using the same underlying processes e.g. action management.

About URM

URM is dedicated to assisting organisations improve their risk management, business continuity and information security in line with leading industry standards such as ISO 31000, ISO 22301 and ISO 27001. It does this through the provision of consultancy, training and Abriska. At all times, the focus is on providing pragmatic and appropriate solutions i.e. getting the balance right.

About Abriska

In addition to Abriska 27036, URM has developed a portfolio of modules to assist organisations undertake risk management activities. These modules include an information security risk management tool (Abriska 27001), business continuity BIA and risk management tool (Abriska 22301) and an enterprise risk management tool (Abriska 31000).

Telephone: 0118 2065 410 **Email:** info@urmconsulting.com **Website:** www.urmconsulting.com

URM, Blake House, Manor Park, Manor Farm Road, Reading, Berkshire, RG2 0JH