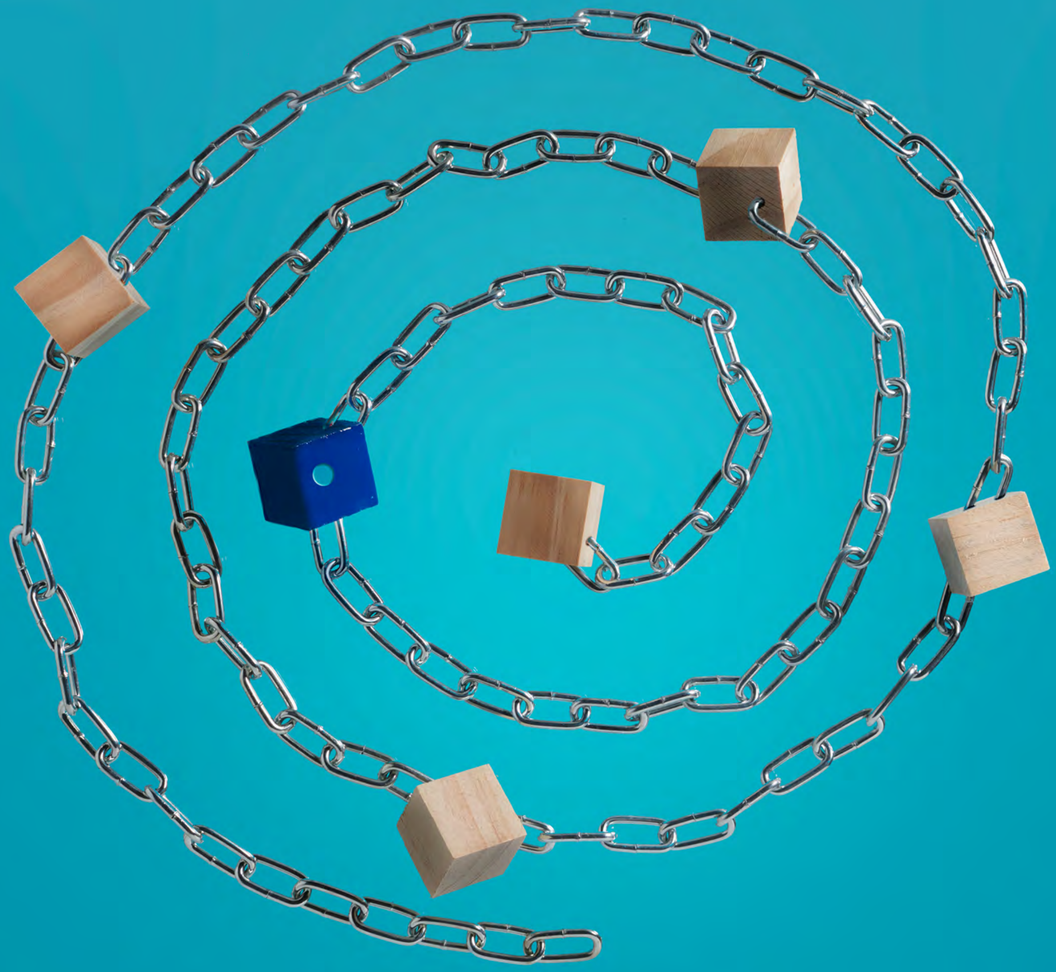
abriska MANAGEMENT

27036

Supplier Risk Management Tool



www.urmconsulting.com

URM

Business **Challenge**

Organisations often struggle with the challenge of conducting supplier due diligence when faced with assessing the information security capabilities of a wide and diverse range of suppliers and partners.

Irrespective of the criticality of a supplier, a single ‘one size fits all’ questionnaire is often sent to all suppliers. As a result, and unsurprisingly, it is inevitable that the questionnaire will lack the required detail for critical suppliers but will be too detailed and inappropriate for low-risk suppliers.

abriska MANAGEMENT

ABRISKA 27036

Methodology **and Key Features**

The core set of questions that form the due diligence have been developed by URM's team of information security and data protection practitioners and are closely aligned to both ISO 27001 and ISO 27036.

With the **Abriska® 27036** software tool, you are able to create and send tailored information security 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 taken from the extensive bank within **Abriska 27036** or designed specifically.

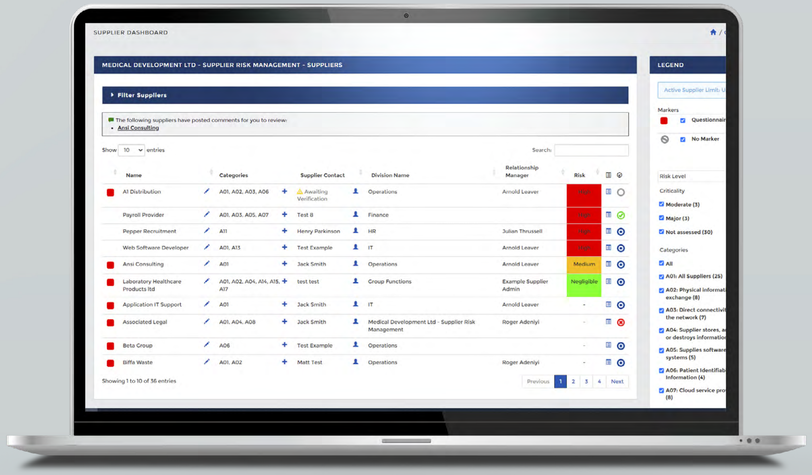
- **Categorisation of Suppliers** – **Abriska 27036** is a single register managing all suppliers assigning both an internal owner and supplier contact. The software comes pre-configured with detailed supplier categories, which are mapped to controls from best practice standards. Additional categories can be easily created by the organisation.

- **Prioritisation of Suppliers** – Each supplier can be prioritised by the information that it has access to by either assessing the confidentiality, integrity or availability of information the supplier can access or by linking an information type through to the supplier. This step ensures that questionnaires, and ultimately, the required controls you expect a supplier to implement, are appropriate to the information being stored, processed or transmitted.

- **Supplier Assessment** – Questionnaires are answered and saved directly into the Abriska interface with your supplier/partner creating a basic account. Your supplier/partner can add additional users to complete the questionnaire where questions can be customised based on business needs and the role of your supplier/partner. Dependant on answers throughout branch questions can be revealed.

- **Reporting and Risk Treatment Actions** – Once the questionnaire has been completed by your supplier/partner, you are notified and are able to analyse the questionnaire responses. The supplier is assigned a risk rating based on their answers and then assigned a priority score. 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.

*With the **Abriska 27036** software tool, you are able to create and send tailored information security questionnaires to any supplier or third party.*



abriska MANAGEMENT

ABRISKA 27036

Key **Benefits**

Proven and 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 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.

Consistent and Repeatable results

Abriska 27036 has been designed to allow your organisation to customise 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.

Flexibility

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.

Maintain Accountability and 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.

abriska MANAGEMENT

Abriska

In addition to Abriska 27036, URM has developed a portfolio of modules to assist organisations implement a best practice approach to managing risk in line with ISO Standards.

These modules a include business continuity BIA and risk management tool (Abriska 22301), an enterprise risk management tool where you can centrally manage all organisational risks (Abriska 31000), an information security risk management tool (Abriska 27001), and an auditing administration tool providing full audit, finding and action management capabilities (Abriska 19011).

Configurable

MODULES

- INFORMATION SECURITY
- SUPPLIERS SECURITY
- AUDIT & TRACKING
- ENTERPRISE RISK MANAGEMENT
- BUSINESS CONTINUITY

abriska MANAGEMENT

Certified to ISO 27001 and ISO 22301, URM is dedicated to assisting organisations improve their information security, risk management and business continuity in line with industry leading standards such as ISO 27001, ISO 31000 and ISO 22301. At all times, the focus is on knowledge transfer and providing pragmatic and appropriate solutions, which meet the requirements of industry standards but are also tailored to an organisation's business objectives and risk appetite, i.e., getting the balance right.

URM Consulting Services Limited
Blake House, Manor Park. Manor Farm Road
Reading, Berkshire
RG2 0JH

T: 0118 206 5410
E: info@urmconsulting.com

www.urmconsulting.com