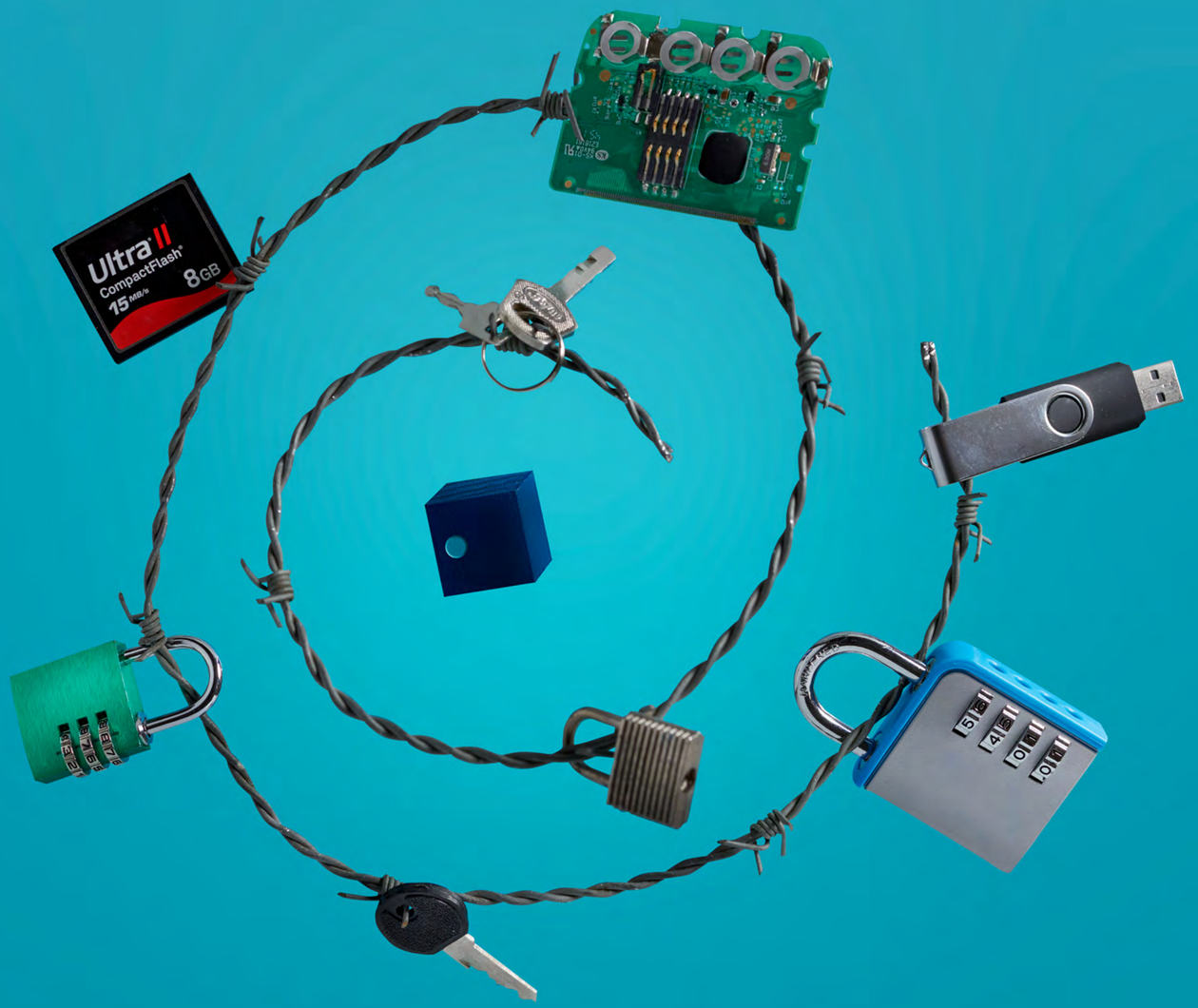
abriska
MANAGEMENT

27001

Information Security Risk Management Tool



www.urmconsulting.com

URM

Business **Challenge**

All organisations face risks to the information that they store and process; these could be due to cyber threats or lack of staff awareness or any number of factors both within and outside of the organisation's control. This is where conducting risk assessments plays such a critical role in understanding which risks are particularly relevant to your organisation and what actions you need to prioritise.

A key feature of Abriska is that it replaces multiple spreadsheets with a 'single source of truth' database. Users are able to enter information through a secure Web-based system, thereby simplifying the risk management process.

abriska MANAGEMENT

ABRISKA 27001

Methodology
and Key Features

Abriska® 27001 aligns with best practice detailed within ISO 27005 and adopts a robust approach to managing information security risk:

- **Asset Identification and Business Impact Analysis** – The first step focusses on determining what information and information processing assets are within scope and what the impact would be following a loss of confidentiality, integrity or availability to these assets.

- **Control Maturity Assessment** – Initially, the control maturity assessment looks at identifying which of the ISO 27001 controls are applicable to your organisation, before assessing the maturity of those applicable controls against a consistent, tailored scale. Abriska has been fully updated in line with the ISO 27002:2022 control set.

- **Risk Assessment** – Abriska assesses risk by determining the likelihood and impact of threats occurring and mapping these against appropriate controls. With the organisation's asset hierarchy in place, risk assessments can be conducted. Abriska is preloaded with mapping between assets, threats and controls – this allows an organisation to quickly identify risks.

- **Reporting** – Having determined information security risks, these can be reported in a number of ways, including displaying how risks have changed over time. All of the mandatory output requirements from ISO 27001 are automatically produced by Abriska, i.e., statement of applicability, risk score matrix, risk treatment plan and risk register.

> ***Abriska 27001*** *utilises a consistent and robust approach to analyse and evaluate risks to information and information processing assets and is totally aligned to meeting the requirements of ISO 27001, as well as complying with best practice risk management as detailed in ISO 31000.*

abriska
MANAGEMENT

A key feature of Abriska is that it replaces multiple spreadsheets with a 'single source of truth' database. Users are able to enter information through a secure Web-based system, thereby simplifying the risk management process.

abriska MANAGEMENT

ABRISKA 27001

Key **Benefits**

Proven and Robust

Abriska 27001 has been used to underpin in excess of 300 certification projects. Abriska automatically produces a range of outputs including the mandatory statement of applicability, risk register and risk treatment plan. The underlying risk assessment methodology has been validated by all the leading UKAS-accredited certification bodies.

Consistent and Repeatable results

Abriska is ideally suited to meeting one of the absolute fundamental requirements of ISO 27001; the need for robust and repeatable risk assessments. The software allows for comparison against previous risk assessments and shows how risks have changed over time. Abriska can also be used to model the potential reduction in risk by implementing various controls or addressing specific vulnerabilities..

Flexibility

The software can be tailored to integrate with other areas of risk management, e.g., aligning with your organisation's risk appetite and strategy. Abriska also allows for varying control implementation across different sites or divisions, with considerable scope for the customisation and the addition of threats and controls, e.g., PCI DSS. The customisation can be implemented directly by the user within the web interface..

Maintain Accountability and Responsibility

Individual areas of Abriska, including risk treatment actions or controls, can be assigned to relevant personnel or teams. Once assigned, users are able to view relevant areas of Abriska depending on their role and privileges within the system. Workflow and notifications ensure that actions are completed within their target dates and risks are updated once completed..

abriska MANAGEMENT

ABRISKA 27001

Abriska

In addition to Abriska 27001, 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 include a business continuity BIA and risk management tool (Abriska 22301), an enterprise risk management tool where you can centrally manage all organisational risks (Abriska 31000), a supplier risk management tool which can help you improve both the effectiveness and efficiency of supplier due diligence (Abrisk 27036) 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