URM Getting the Balance Right

Abriska 27001 Migration from 2013 to 2022 Version of ISO 27001

Prepared for:

Abriska Clients

1.0 Preface

1.1 Prepared By

Name	Function
Skwarka, Jacqueline	Customer Success Manager

1.2 Reviewed and Authorised By

Name	Function
Matt Thomas	Director

1.3 Contact Details

Address	Telephone
Blake House Manor Park Manor Farm Road Reading Berkshire RG2 0JH	0118 206 5410

1.4 Change History

Version	Date	Revision Description
0.1	4 October 2022	Initial Draft
0.2	27 January 2023	Draft Update
1.0	15 February 2023	Final Draft

Contents

2.0 Abriska Migration from ISO 27001:2013 to ISO 27001:2022

Further to the release of ISO 27001:2022, the purpose of this update is to outline the Abriska migration plan from ISO 27001:2013 to ISO 27001:2022.

2.1 Methodology

The Abriska methodology remains conformant to the requirements of ISO 27001:2022The latest version of Abriska has been updated in line with the ISO 27001:2022 Annex A controls which better reflect today's security challenges and threats. Abriska 27001 also continues to align with best practice as detailed in ISO 27005, with the tool utilising an asset-based approach.

The Abriska tool has been updated to allow you to take advantage of the 'attribute' features which were introduced by the 2022 version of the Standard. This functionality provides you with different perspectives for viewing controls so that it is easier for you to discern whether you need controls or not, and better appreciate the spread of control maturity within each attribute which may assist in reducing risk.

2.2 Changes to Abriska

2.2.1 Controls

The Annex A controls within ISO 27001:2022 have been updated as per the changes made to ISO 27002:2022 in February 2022. Annex A now contains 93 controls as opposed to 114 contained within ISO 27001:2013. The controls are now listed under 4 themes: Organisational, Technological, Physical and People.

As the new Standard reflects the rapid growth of digital technology and the changing nature of threats over time, some of the controls have been merged, some deleted, and 11 new controls have been introduced.

As part of the risk treatment process, you will need to 'determine all controls that are necessary…' and then compare this list with the controls in ISO 27001:2022 Annex A to 'verify that no necessary controls have been omitted'. 'Note 1' attached to the mandatory risk treatment clause (6.1.3) states that 'Organisations can design controls as required, or identify them from any source'. URM has mapped the 2013 controls with the 2022 controls identifying those that are new, those that have been deleted and those that have been merged, clarified, extended or replaced. In Appendix A of this document, we have produced a table showing the mapping of 2013 to 2022 controls for your reference.

2.3 Timeline for Proposed Changes

URM has enhanced Abriska to reflect the changes in ISO 27001:2022 to ensure that the tool remains compliant with the Standard This version has been released into the main live environment; however, you will have the option of deciding when to migrate to the new version.

Included as part of the annual maintenance, URM will address with you a timeline for migrating from the current Abriska version and provide training to all users on how to use new functionality such as the attributes.

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

1. **'Reset'** - This will involve deleting all control maturity assessments, adding the new controls and new threat mapping. You will then be responsible for undertaking a control maturity assessment of all 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 2013 – 2022 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. You will be responsible for reviewing and verifying the migrated maturity assessments and evaluating any new controls.
3. **'Bespoke'** – Any specific requirements you have can be discussed including quoting for additional support.

To discuss your queries please email jskwarka@urmconsulting.com or your account manager.

3.0 Appendix A: ISO 27002: 2013 to ISO 27002:2022 Mapping

ISO 27002:2022 control reference	ISO 27002:2013 control reference	Control name
5.1	5.1.1, 5.1.2	Policies for information security
5.2	6.1.1	Information security roles and responsibilities
5.3	6.1.2	Segregation of duties
5.4	7.2.1	Management responsibilities
5.5	6.1.3	Contact with authorities
5.6	6.1.4	Contact with special interest groups
5.7	New	Threat intelligence
5.8	6.1.5, 14.1.1	Information security in project management
5.9	8.1.1, 8.1.2	Inventory of information and other associated assets
5.10	8.1.3, 8.2.3	Acceptable use of information and other associated assets
5.11	8.1.4	Return of assets
5.12	8.2.1	Classification of information
5.13	8.2.2	Labelling of information
5.14	13.2.1, 13.2.2, 13.2.3	Information transfer
5.15	9.1.1, 9.1.2	Access control
5.16	9.2.1	Identity management
5.17	9.2.4, 9.3.1, 9.4.3	Authentication information
5.18	9.2.2, 9.2.5, 9.2.6	Access rights
5.19	15.1.1	Information security in supplier relationships
5.20	15.1.2	Addressing information security within supplier agreements

ISO 27002:2022 control reference	ISO 27002:2013 control reference	Control name
5.21	15.1.3	Managing information security in the ICT supply chain
5.22	15.2.1, 15.2.2	Monitoring, review and change management of supplier services
5.23	New	Information security for use of cloud services
5.24	16.1.1	Information security incident management planning and preparation
5.25	16.1.4	Assessment and decision on information security events
5.26	16.1.5	Response to information security incidents
5.27	16.1.6	Learning from information security incidents
5.28	16.1.7	Collection of evidence
5.29	17.1.1, 17.1.2, 17.1.3	Information security during disruption
5.30	New	ICT readiness for business continuity
5.31	18.1.1, 18.1.5	Legal, statutory, regulatory and contractual requirements
5.32	18.1.2	Intellectual property rights
5.33	18.1.3	Protection of records
5.34	18.1.4	Privacy and protection of PII
5.35	18.2.1	Independent review of information security
5.36	18.2.2, 18.2.3	Compliance with policies, rules and standards for information security
5.37	12.1.1	Documented operating procedures
6.1	7.1.1	Screening
6.2	7.1.2	Terms and conditions of employment
6.3	7.2.2	Information security awareness, education and training
6.4	07.2.3	Disciplinary process
6.5	07.3.1	Responsibilities after termination or change of employment
6.6	13.2.4	Confidentiality or non-disclosure agreements

ISO 27002:2022 control reference	ISO 27002:2013 control reference	Control name
6.7	06.2.2	Remote working
6.8	16.1.2, 16.1.3	Information security event reporting
7.1	11.1.1	Physical security perimeters
7.2	11.1.2, 11.1.6	Physical entry
7.3	11.1.3	Securing offices, rooms and facilities
7.4	New	Physical security monitoring
7.5	11.1.4	Protecting against physical and environmental threats
7.6	11.1.5	Working in secure areas
7.7	11.2.9	Clear desk and clear screen
7.8	11.2.1	Equipment siting and protection
7.9	11.2.6	Security of assets off-premises
7.10	08.3.1, 08.3.2, 08.3.3, 11.2.5	Storage media
7.11	11.2.2	Supporting utilities
7.12	11.2.3	Cabling security
7.13	11.2.4	Equipment maintenance
7.14	11.2.7	Secure disposal or re-use of equipment
8.1	6.2.1, 11.2.8	User endpoint devices
8.2	9.2.3	Privileged access rights
8.3	9.4.1	Information access restriction
8.4	9.4.5	Access to source code
8.5	9.4.2	Secure authentication
8.6	12.1.3	Capacity management
8.7	12.2.1	Protection against malware

ISO 27002:2022 control reference	ISO 27002:2013 control reference	Control name
8.8	12.6.1, 18.2.3	Management of technical vulnerabilities
8.9	New	Configuration management
8.10	New	Information deletion
8.11	New	Data masking
8.12	New	Data leakage prevention
8.13	12.3.1	Information backup
8.14	17.2.1	Redundancy of information processing facilities
8.15	12.4.1, 12.4.2, 12.4.3	Logging
8.16	New	Monitoring activities
8.17	12.4.4	Clock synchronization
8.18	9.4.4	Use of privileged utility programs
8.19	12.5.1, 12.6.2	Installation of software on operational systems
8.20	13.1.1	Networks security
8.21	13.1.2	Security of network services
8.22	13.1.3	Segregation of networks
8.23	New	Web filtering
8.24	10.1.1, 10.1.2	Use of cryptography
8.25	14.2.1	Secure development life cycle
8.26	14.1.2, 14.1.3	Application security requirements
8.27	14.2.5	Secure system architecture and engineering principles
8.28	New	Secure coding
8.29	14.2.8, 14.2.9	Security testing in development and acceptance
8.30	14.2.7	Outsourced development

ISO 27002:2022 control reference	ISO 27002:2013 control reference	Control name
8.31	12.1.4, 14.2.6	Separation of development, test and production environments
8.32	12.1.2, 14.2.2, 14.2.3, 14.2.4	Change management
8.33	14.3.1	Test information
8.34	12.7.1	Protection of information systems during audit testing