

ISMS SCOPE DOCUMENT

Change history

Date	Revision	Changes By	Details of Changes
April 5, 2018	0.1	V. Finkinshtein	Created, basic document outline
August 30, 2018	0.2	V. Finkinshtein	Edited
Nov 30, 2018	1.0	J. Patterson	Approved
Dec 5, 2018	2.0	J. Patterson	Included Scope Statement, Approved

Table of Contents

Change history	1
1. Purpose, scope and users	2
2. Reference documents.....	2
3. Definition of ISMS scope.....	2
3.1. Processes and services	3
Core.....	3
Perspective (PSV)	3
GRC Cloud.....	3
WRM.....	3
GAL.....	3
RiskVision	3
3.2. Organizational units	3
3.3. Locations.....	3
3.4. Networks and IT infrastructure.....	3
3.5. The following outsourced vendors may impact the information security as it relates to the scope of certification:.....	3

4. Validity and document management..... 4

1. Purpose, scope and users

The purpose of this document is to clearly define the boundaries of the Information Security Management System (ISMS) in Resolver Inc..

The ISMS covers the development, hosting and supporting activities for Resolver’s Integrated Risk Management applications comprised of Risk and Incident Management, Audit, Compliance, Internal Controls, Business Continuity and Emergency Management, IT Risk and Compliance and Vulnerability Management

Specifically, the following products are included in the ISMS:

1. Resolver Core application (SaaS)
2. Perspective application (SaaS)
3. GRC Cloud application (SaaS)
4. RiskVision application (SaaS)
5. Global AlertLink application (SaaS)
6. WRM application (SaaS)

This document is applied to all documentation and activities within the ISMS.

Users of this document are members of Resolver Inc management, members of the project team implementing the ISMS:

CISO, Information Security Team members, DevOps Team members, IT department team members.

2. Reference documents

- ISO/IEC 27001 standard, clause 4.3
- List of legal, regulatory, contractual and other requirements

3. Definition of ISMS scope

The organization needs to define the boundaries of its ISMS in order to decide which information it wants to protect. Such information will need to be protected no matter whether it is additionally stored, processed or transferred in or out of the ISMS scope. The fact that some information is available outside of the scope doesn't mean the security measures won't apply to it – this only means that the responsibility for applying the security measures will be transferred to a third party who manages that information.

Taking into account the legal, regulatory, contractual and other requirements, the ISMS scope is defined as specified in the following items:

3.1. Processes and services

Core

- Resolver Core application (SaaS)
- All available in AWS production environments

Perspective (PSV)

- Perspective application (SaaS)
- All available in AWS production environments

GRC Cloud

- GRC Cloud application (SaaS)
- All available in AWS production environments

WRM

- WRM application (SaaS)
- All available in AWS production environments

GAL

- All available in AWS production environments
- Global AlertLink application (SaaS)

RiskVision

- All available in Rackspace production environments
- RiskVision application (SaaS)

3.2. Organizational units

Development, DevOps, HR, Customer Success, Legal, Information Security, Information Systems (IT).

3.3. Locations

111 Peter St, Suite 804, Toronto, ON, M5V 2H1

3.4. Networks and IT infrastructure

Toronto Office network infrastructure

3.5. The following outsourced vendors may impact the information security as it relates to the scope of certification:

VENDOR NAME	DESCRIPTION OF SERVICE(S) PROVIDED
AWS	Cloud Service Provider, hosting
Rackspace	Cloud Service Provider, hosting

4. Validity and document management

This document is valid as of April 2018.

The owner of this document is CISO who must check and, if necessary, update the document at least once a year.

When evaluating the effectiveness and adequacy of this document, the following criteria need to be considered:

- number of incidents arising from unclear definition of the ISMS scope
- number of corrective actions taken due to an inadequately defined ISMS scope
- time put in by employees implementing the ISMS to resolve dilemmas concerning the unclear scope



James Patterson
COO, CISO
Resolver

COO and CISO

James Patterson.



CEO

Will Anderson