

Issue 1.0, December 2006

The information in this note applies to:

## RuleSafe 2.x (all builds)

**This note describes how RuleSafe™ can be used as part of an Information Security Management System (ISMS) as defined by International Standard ISO 27001. It also shows how you can use RuleSafe to manage an ISMS project to achieve conformity with ISO 27001.**

This note assumes you are familiar with information security standards such as ISO/IEC 27001:2005 (referred to as ISO 27001 in this note) or its predecessors such as BS 7799-2:2002.

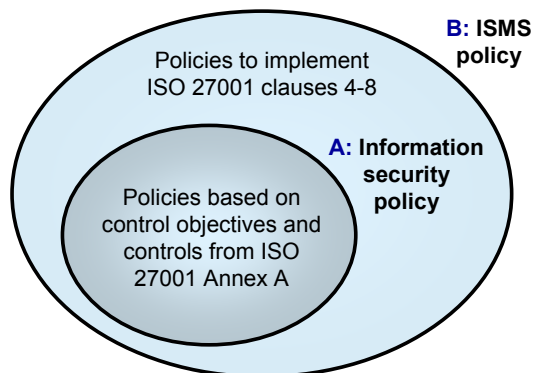
[References to ISO 27001 are in brackets].

### Introduction

ISO 27001 has two main aspects. It specifies how an organisation establishes, implements and maintains an ISMS [4, 5, 6, 7, 8]. It also specifies how to implement security controls that are tailored to the needs of the organisation, based on a standard set of controls [Annex A].

ISO 27001 requires that the organisation defines an **ISMS policy**, to set out its overall framework for information security and risk management. Part of the ISMS policy is the organisation's **information security policy** [4.2.1b].

RuleSafe is designed to be the vehicle for establishing and achieving awareness of an information security policy. You can also use it to specify and track ISMS-related responsibilities throughout the Plan-Do-Check-Act lifecycle, storing all necessary evidence of ISO 27001 conformity.



The following sections describe how RuleSafe supports these two types of policy.

### A: Information Security Policy and the Statement of Applicability

ISO 27001 requires that control objectives and controls are selected, appropriate for the needs of the organisation [4.2.1g].

RuleSafe supports this by allowing you to create a comprehensively documented set of controls, held as a

'policy set', which are cross-referenced to the individual statements in ISO 27001 Annex A and other sources.

RuleSafe also enables you to create a **Statement of Applicability** [4.2.1j] and demonstrate how your internal policies cover the selected parts of ISO 27001 Annex A.

Publishing the selected controls in RuleSafe, with supporting guidance and easily searchable by employees according to their role, helps you meet ISO 27001's requirements for training and awareness [5.2.2].

### B: ISMS Policy and achieving ISO 27001

In addition to holding the information security policy, RuleSafe can also manage the higher-level policies concerned with establishing, implementing and maintaining the ISMS.

These policies are created in RuleSafe and cross-referenced with the mandatory ISO 27001 clauses 4-8. They comprise the organisation's specific approach to the ISMS, including any forms or templates for activities such as management approvals [4.2.1h, i] and risk assessments [4.2.1c]. You can group these higher-level ISMS policies into a distinct RuleSafe 'policy set', to target them at the people responsible for implementing the ISMS, and to obtain a scorecard of progress towards ISMS completion.

RuleSafe's role-based approach to policy definition ensures each ISMS-related action is clearly communicated to those responsible for it.

Using RuleSafe's ability to link policies to process phases, individual ISMS policy statement can be linked to the correct phase of the Plan-Do-Check-Act cycle. This enables easy access to the activities relevant to the currently active phase.

RuleSafe's compliance tracking features enable you to record in one system all evidence of ISMS activities that are complete, and prepare for certification if desired.

### Creating your ISO 27001 framework with RuleSafe

You can use RuleSafe as the repository and portal for all your ISMS documentation and evidence of conformity.

Sample ISMS documentation and information security policies are available from Secoda's solutions partners. RuleSafe can be supplied with this material pre-loaded, substantially cutting the time need to establish an ISMS. Contact us for details.

### For more information

To learn more about how RuleSafe can accelerate your ISO 27001 initiative, email [info@secoda.com](mailto:info@secoda.com) or telephone **+44 (0)20 7232 4877**, or contact a Secoda solutions partner – see [www.secoda.com/partners.htm](http://www.secoda.com/partners.htm).