

# CRAMM 5.1 EN

## INFORMATION SECURITY TOOLSET

It is increasingly recognised that risk analysis and management, despite their critical importance, are unsustainable without effective tools that can make the process efficient too.

CRAMM Version 5 is today's most comprehensive, most award winning and widely adopted method for information security risk analysis and management. CRAMM Version 5 can do everything described below and more besides.

With over 600 deployed copies in 25 countries and 20 business sectors it has been extensively proven, including in support of programme delivering formal certification against ISO/IEC 27001 and by many national security authorities as the recognised Best Practice for Information Security Management.

It is the 'benchmark' against which all other methods are evaluated and routinely wins assessments of 'value for money', reflecting the significant development investments made by such organisations as the UK Government and NATO.

### Information Risks Analysis and Management fully compliant with ISO/IEC 27001 and ISO/IEC 27002

#### CRAMM controls database

The CRAMM Version 5 controls database is hugely valuable in its own right. It covers the latest best practice in all aspects of security including technical, physical, personnel, documentation and procedural controls. CRAMM contains a library of 3500 countermeasures that completely comply with ISO/IEC 27002:2005.

#### Security inspection

The security inspection or review process is carried out in support of a number of objectives, for example:

- ◆ to ensure that the required minimum standards are applied and continue to be applied;
- ◆ to maintain an organisation's focus on the importance of security;
- ◆ as part of an ongoing security education and awareness programme.

#### Risk assessment tools

CRAMM includes comprehensive risk assessment tools which are fully compliant with ISO/IEC 27001 and ISO/IEC 27002, including:

- ◆ Asset dependency modelling
- ◆ Business impact assessment
- ◆ Assessing threats and vulnerabilities
- ◆ Assessing levels of risk
- ◆ Identifying required and justified controls on the basis of the risk assessment.

#### ISO/IEC 27001 and ISO/IEC 27002 compliance tools

CRAMM is a well-proven methodology to assist organisations to assess their compliance with the ISO/IEC 27001 and then take the actions to achieve compliance. Key components of this methodology are incorporated into CRAMM, including wizards for:

- ◆ Defining the scope of the Information Security Management System (ISMS)
- ◆ Defining the management framework
- ◆ Conducting a Gap Analysis, following the 'Plan, Do, Check, Act' principles
- ◆ Preparing a Security Improvement Programme
- ◆ Producing a Statement of Applicability
- ◆ Producing an Information Asset Register
- ◆ Producing the risk assessment and risk treatment documents.

#### Pro-forma security policies and other security documentation

CRAMM Version 5 contains pro-forma documents and 'wizards' to help the user create a wide range of completed security documentation.

#### Business continuity tools

CRAMM provides tools to support the following key processes in business continuity management and is entirely consistent with the IT Infrastructure Library (ITIL) and Business Continuity Institute (BCI) standards on business continuity