CRAMM v5.1 Information Security Toolkit

Risk assessments should identify, quantify, and prioritise risks against criteria for risk acceptance and objectives relevant to the organisation. The results should guide and determine the appropriate management action and priorities for managing information security risks and for implementing controls selected to protect against these risks.

BS7799: 2005

We all face risks everyday – ranging from the mundane, such as "which way shall I drive to work today?" to risks which can affect the rest of our lives, like "shall I apply for that job?" – Risk is something we all live with and feel we practice and understand.

In the Information Systems environment, new business practices – such as outsourcing, partnerships and consortiums – and new technologies, such as remote working, wireless LANs and PDAs, mean that we are constantly facing new threats and risks, and the need for additional controls.

These complexities make it practically impossible for an Information Security Officer to keep up to date without automated support and CRAMM has, for many years, been the UK Government's preferred approach to risk assessment. Now Insight has further enhanced CRAMM by incorporating its knowledge base from hundreds of worldwide consultancy assignments, including many successful certifications against BS7799.

CRAMM v5.1 provides fantastic value for money, and with over 600 copies of CRAMM already in use in 23 countries, CRAMM is exceedingly well proven. Supported by Insight Consulting's wide range of services, users of CRAMM have an indispensable aid for the delivery of the 'benchmark good practice', set by the Information Security Forum.

Understanding risk

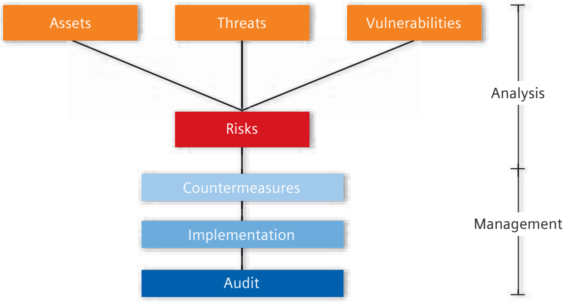
Corporate Governance, Turnbull and BS7799: 2005/ISO 27001 all require that a sound understanding of the risk of information assets is obtained and maintained. To do this you need to combine together a complex set of 'risk components', including:

- Over 400 types of asset
- More than 25 different types of impact
- 38 types of threat
- Seven different measures of risk
- A countermeasure library containing more than 3,500 detailed, but generic, controls

SIEMENS

Global network of innovation

Insight Consulting



Insight's CRAMM methodology

A complex but critical process

With this understanding it is possible to answer the many questions that arise each day in respect of information security, such as:

- What security requirements should we include in this managed service agreement?
- Are there implications from allowing our users to connect to the Internet?
- How can we demonstrate to the BS7799 auditors that our risks have been managed properly?

Acceptance not avoidance

Managing risk is a matter of 'Risk Treatment' under which risks are reduced to an acceptable level and not 'avoided' by either ignoring them or trying to remove them altogether. Risk management processes include activities such as:

- Identifying requirements for specific controls such as Smart Cards
- Demonstrating compliance with legislation
- Developing a business continuity strategy
- Developing a security policy for a new system
- Auditing the status of security controls on an existing system

Secure change management

As the pace of change accelerates ever faster, the key challenge is to be able to build security into new systems as they arise. This requires a fast and effective approach and the capability to interrogate results, as well as adapt the risk assessment as new details become available.

An indispensable information security toolkit

CRAMM v5.1 is today's most comprehensive and widely adopted method for information security, risk analysis and management. It is the 'benchmark' against which all other methods are evaluated, reflecting the significant development investments made by such organisations as the UK Government and NATO.

CRAMM v5.1 provides a comprehensive risk assessment method with the ability to carry out three different types of review: CRAMM Express Reviews; BS7799: 2005 Reviews; and CRAMM Expert Reviews.

CRAMM supports many additional functions including:

- BS7799: 2005 Compliance
- Production of Security Documentation
- Investigation against Standards
- Recording information required for Business Continuity Planning

CRAMM contains:

- A database consisting of over 3,500 security controls covering all aspects of information security
- A set of tools to support you in achieving certification or compliance against BS7799: 2005
- Pro-forma information security policies, security operating procedures and other useful security documentation
- Pre-defined risk assessments covering generic information systems – such as payroll
- A complete set of risk management help tools, to support your security improvement planning and make the most of your information security budgets

Other additions in CRAMM v5.1 include:

- Updated mapping of the CRAMM Countermeasures to reflect the BS7799: 2005/ISO 27001 controls
- Graphical reports for countermeasures
- Security Resource checklists
- Enhancements for reporting functionality with CRAMM Express
- A 'Copy and Compare' tool that allows users to copy information from one review to another and produce comparisons

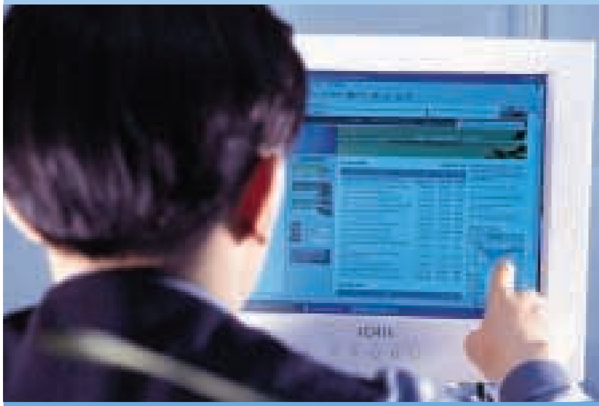
For further information about CRAMM please visit **http://www.cramm.com**

CRAMM V
Information Security Toolkit

Insight Consulting has launched an updated version of the most comprehensive and widely adopted method for information security risk analysis and management, CRAMM.

The new version provides support for:

- ISO 27001
- Security inspections
- Recording compliance against industry standards for UNIX and Windows XP operating systems
- Creation of security operating procedures



Insight Consulting is the specialist security, compliance and continuity unit of Siemens Communications and offers a complete, end-to-end portfolio encompassing:

- Research
- Consultancy
- Testing
- Implementation
- Training
- Recruitment
- Managed services

Insight is BS7799 certified, is a GCat and S-Cat (Category 7) supplier and subscribes to the CESG Listed Advisor Scheme (CLAS) and CHECK services.

If you'd like to discuss how Insight could help you manage risk in your organisation, email us at **insight@insight.co.uk** or visit our web site at **www.siemens.co.uk/insight**

Insight Consulting
Churchfield House
3 The Quintet
Churchfield Road
Walton on Thames
Surrey KT12 2TZ
United Kingdom

Tel: +44 (0)1932 241000
Fax: +44 (0)1932 236868
www.cramm.com