



Instituting a security policy for your organization is far more than just a matter of buying firewalls and installing anti-virus software. Far too many companies believe that the best way to protect themselves is to throw vast amounts of money into security technology, and leave it at that, forgetting that true security can begin somewhere as blindingly obvious – and as frequently overlooked – as preventing tailgating or keeping windows locked! It is also vitally important to ensure that levels of security are correct at every different point in the organization: there is little sense in spending a fortune on protecting the network with layers of software, only to make it difficult for employees to actually do their jobs.

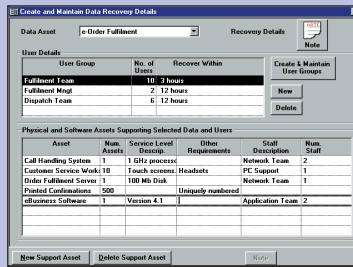
The best way of creating a security policy that is tailored to your business is to perform a detailed risk assessment of all areas and all levels of the organization, but many companies are put off doing that because they believe it to be too complex to achieve in-house, and too expensive to outsource. Which is where *CRAMM* comes in. *CRAMM* is an application that leads you through every aspect of risk analysis and assessment, producing a set of detailed reports and recommendations at the end of it.

*CRAMM* has a very interesting – and very aristocratic – pedigree. It was initially developed by the CCTA (now the U.K. Office of Government Commerce) as the preferred method of risk assessment for government departments and organizations wishing to do business with the government, and originally stood for CCTA risk analysis management method. Now developed and supported by Insight Consulting, it is still the preferred tool for risk assessment for a number of very high-profile bodies, such as the police, the U.K. National Health Service, NATO and all areas of U.K. government.

Although *CRAMM* is a product, it is the methodology that the product enforces that is more important. Just as BS5750/ISO9001 was the watchword for the 1990s, there can be very few companies today that are unaware of BS7799, the British standard which defines best practice for information security. The *CRAMM* methodology fully supports the five stages of BS7799 accreditation, ensuring that once you have performed a *CRAMM* risk assessment, you can demonstrate compliance to a BS7799 auditor. *CRAMM* will also ensure that you are complying with other legislation, such as the U.K.'s newly-toughened *Data Protection Act*.

A *CRAMM* review is carried out in three stages, and the product takes you through the stages logically and effortlessly. The first stage is to define the existing business, inventory all assets, and build a model of your organization. In the second stage, you relate each asset or group

# CRAMM



by Craig Hinton

**Version:** 4

**Supplier:** Insight

**Price:**

*Commercial Company:* £2,800 (plus £850 yearly maintenance and service agreement)

*Listed SCAT Company:* £1,600 (plus £850 yearly maintenance and service agreement)

*U.K. Government Depts/Agencies:* £600 (plus £850 yearly maintenance and service agreement)

**Contact:** +44 (0)1932 236898

cramm@insight.co.uk

www.insight.co.uk

**FOR** An excellent and straightforward way of performing a risk assessment on all aspects of corporate security, *CRAMM* ensures that no stone remains unturned.

**AGAINST** None.

**VERDICT** For those of you who think a risk assessment too expensive, time-consuming or complex, *CRAMM* will make you think again.

Features	★★★★★
Ease of use	★★★★★
Performance	n/a
Documentation	★★★★★
Support	★★★★★
Value for money	★★★★★
<b>Overall Rating</b>	<b>★★★★★</b>

**For those of you who think a risk assessment too expensive, time-consuming or complex, CRAMM will make you think again.**

Contact Information:



Insight Consulting Limited, Churchfield House,  
5 The Quintet, Churchfield Road,  
Walton on Thames, Surrey. KT12 2TZ

© Copyright West Coast Publishing 2001

of assets to possible threats, assess the vulnerabilities and measure the risk. The final stage allows you to define countermeasures based on the first two stages and produce a list of recommendations.

At the heart of *CRAMM* is the Controls Database. This contains over 3,000 security controls that have been defined by security agencies and standards bodies. For each control, the database describes where the control would be appropriate, its cost and effectiveness, and also whether it reduces the threat of security breaches, reduces the impact of any breach, detects it, or simply enables faster recovery. From this, you can determine whether it is worth spending a lot of money securing an area of the business that is not vital, or whether you can truly take the risk of enforcing a lower level of security if the area is less important to the business. Basically, you are balancing the cost of protection against the cost of a threat, so money is spent only where it is needed – and this can be justified through the *CRAMM* methodology.

Because of this, systems and security administrators also have another reason to like *CRAMM*: after years of attempting to justify spending on new security hardware and software based on vague or unsubstantiated estimates, they can now present the person who signs the checks with quantitative as well as qualitative data. Furthermore, extensive 'what-if' capabilities mean that different risk scenarios can be proposed and evaluated.

At this point, many of you are probably thinking that a product that can do all of this must be hellishly difficult to use. But nothing could be further from the truth. *CRAMM* is simplicity itself to install (it does require a dongle to work, adding an extra level of security to the product itself), and the hierarchical structure of the menus mean that a complete risk analysis and assessment of your business becomes a straightforward matter of proceeding from one window to another. And, at the end of an assessment, *CRAMM* will provide you with detailed reports and charts, which can themselves be tailored to suit your precise needs.

If you need help, a comprehensive set of wizards is provided, as well as extensive online help. A number of pre-defined risk models are also on offer, allowing you the option of taking one of them and tailoring it to fit your own organization. And if that isn't enough, Insight offers training, assistance and consulting if you are still having trouble.

*CRAMM*'s popularity is backed up by the figures: over 300 organizations use *CRAMM* in 20 countries. It was also used as the benchmark for the British Standards Institution's guidance on risk assessment, which is high praise indeed! And as a straightforward yet extremely comprehensive tool for performing risk analysis and assessment in any organization, the product is without compare – there really isn't anything approaching it on the market today. If you want to ensure that there are no cracks in your organization's security policy, and that you are protected to the correct degree and the correct standards at every level of the business, *CRAMM* is definitely the product for you.

