itSM Solutions® DITY™ Newsletter Reprint

This is a reprint of an itSM Solutions® DITY™ Newsletter. Our members receive our weekly DITY Newsletter, and have access to practical and often entertaining articles in our archives. DITY is the newsletter for IT professionals who want a workable, practical guide to implementing ITIL best practices -- without the hype.

become a member

(It's Free. Visit http://www.itsmsolutions.com/newsletters/DITY.htm)

Publisher
itSM Solutions™ LLC
31 South Talbert Blvd #295
Lexington, NC 27292
Phone (336) 510-2885
Fax (336) 798-6296

Find us on the web at: http://www.itsmsolutions.com.
To report errors please send a note to the editor, Hank Marquis at hank.marquis@itsmsolutions.com
For information on obtaining copies of this guide contact: sales@itsmsolutions.com
Copyright © 2006 Nichols-Kuhn Group. ITIL Glossaries © Crown Copyright Office of Government Commerce. Reproduced with the permission of the Controller of HMSO and the Office of Government Commerce.

Notice of Rights / Restricted Rights Legend
All rights reserved. Reproduction or transmittal of this guide or any portion thereof by any means whatsoever without prior written permission of the Publisher is prohibited. All itSM Solutions products are licensed in accordance with the terms and conditions of the itSM Solutions Partner License. No title or ownership of this guide, any portion thereof, or its contents is transferred, and any use of the guide or any portion thereof beyond the terms of the previously mentioned license, without written authorization of the Publisher, is prohibited.

Notice of Liability
This guide is distributed "As Is," without warranty of any kind, either express or implied, respecting the content of this guide, including but not limited to implied warranties for the guide's quality, performance, merchantability, or fitness for any particular purpose. Neither the authors, nor itSM Solutions LLC, its dealers or distributors shall be liable with respect to any liability, loss or damage caused or alleged to have been caused directly or indirectly by the contents of this guide.

Trademarks
itSM Solutions is a trademark of itSM Solutions LLC. Do IT Yourself™ and DITY™ are trademarks of Nichols-Kuhn Group. ITIL ® is a Registered Trade Mark, and a Registered Community Trade Mark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office, and is used here by itSM Solutions LLC under license from and with the permission of OGC (Trade Mark License No. 0002). IT Infrastructure Library ® is a Registered Trade Mark of the Office of Government Commerce and is used here by itSM Solutions LLC under license from and with the permission of OGC (Trade Mark License No. 0002). Other product names mentioned in this guide may be trademarks or registered trademarks of their respective companies.

IT Experience. Practical Solutions.

DITY™ Newsletter

The workable, practical guide to Do IT Yourself™

Syndicate!

10 STEPS TO DO IT YOURSELF CRAMM

Vol. 2.8, feb. 22, 2006

hank MARQUIS

Articles
E-mail
Bio

By Hank Marquis

The *IT Infrastructure Library* (ITIL®) promotes the *CCTA Risk Analysis and Management Method* (CRAMM) for risk assessment. Everyone agrees managing risk is critical, yet few actually use CRAMM or any other formal system!

Part of the reason for this is that CRAMM is a sophisticated software tool that requires a trained practitioner to operate. However, if you examine CRAMM, you soon realize you can obtain many of the benefits without investing in consultants or expensive software solutions.

CRAMM is simply a process template for analyzing risks (*threats* an *asset* faces due to *vulnerabilities*) and then managing those risks through countermeasures. While CRAMM software includes over 3,000 countermeasures in its database -- something you don't get doing CRAMM yourself -- you can still achieve sound risk assessments.

Following I will explain CRAMM goals, methods, techniques and applications; then I will show how to gain many CRAMM benefits in a matter of minutes -- for very low cost.

CRAMM provides a framework to calculate risk from asset values and vulnerabilities,

referred to as Risk Analysis. The framework also helps you avoid, reduce, or choose to accept these risks, referred to as Risk Management.

The idea is that by analyzing assets one can realize the potential damage caused by a failure in Confidentiality (unauthorized disclosure), Integrity (unauthorized modification or misuse) or Availability (destruction or loss). CRAMM supposes that it is cost prohibitive to eliminate risk; but that you can cost effectively mitigate risk by structured analysis of assets.

CRAMM follows a rigid format. CRAMM:

- Uses meetings, interviews, and questionnaires for data collection.
- Identifies and categorizes IT assets into one of three categories: 1) data, 2) application/software 3) physical assets (equipment, buildings, staff, etc.)
- Requires you to consider the Impact of the loss of *Confidentiality, Integrity and Availability* (CIA) of the asset.
- Expresses Vulnerability (the likelihood that a threat may occur) as: very high, high, medium, low or very low.
- Expresses Risk (the likelihood that a threat could exploit the Vulnerability) as: high, medium or low.

CRAMM has three stages:

1. Asset identification and valuation. The goal here is to identify and value assets.
2. Threat and vulnerability assessment. The goal here is to assess the CIA risks to assets.
3. Countermeasure selection and recommendation. The goal here is to identify the changes required to manage the CIA risks identified.

Risk Assessment comprises stage 1, and about half of stage 2; **Risk Management** the balance of stage 2 and stage 3. At each stage there is discussion and agreement with appropriate level management. This is where awareness builds in management of the issues. One of the most difficult aspects of risk management is justifying the costs involved, which may be very high. Traditional cost vs. benefit analysis does not work well for security, and CRAMM provides a clearer method for showing the potential cost to an organization. CRAMM also involves the entire organization (management, IT staff and Customers) in the process, creating buy-in and acceptance of the result of your assessment.

The Manual CRAMM

Without the CRAMM software, you can approximate a CRAMM session using some paper, pencils, office tools like spreadsheets and word processors, the knowledge of your staff, the security Incidents that have occurred, and of course, news about the latest hacker exploits.

The following assessment process is based on CRAMM tenets, but does not provide the same level of detail, control, or options as the CRAMM software. On the other hand, you wont spend thousands of dollars and you will still find it capable and valuable! Figure 1 shows the results of a completed “Manual CRAMM” assessment.

Asset Owner: H. Marquis **Asset:** Credit Card Data							
	CONFIDENTIALITY public (0), restricted (1-5), confidential (6-9), secure (10)			**INTEGRITY** low (1-3), moderate (4-7), high (8-9, very high (10)		**AVAILABILITY** low (1-3), moderate (4-6), high (7-8), very high (9), mandatory (10)	
Impact Requirement (1-10)	10 / secure			10 / very high		8 / high	
Threats *list all that apply*	**Disclosure**	**Theft**	**Loss**	**Hacking**	**input errors**	**Drive failure**	**Power Failure**
Vulnerability (1-10) *none (0), low (1-4), moderate (5-7), high (8-9), very high (10)*	10	3	1	8	2	5	2
Threat (1 to 100) *Impact X Vulnerability*	100	30	10	80	20	40	16
Risk Level *Low (1-33), Medium (34-67), High (68-100)*	High	Low	Low	High	Low	Medium	Low
Countermeasures *list all that apply*	Password protection			Firewall	Data input forms Data validation		

Figure 1. Example Manual "CRAMM" Grid

Following is a 10-step plan that involves IT staff and the Business, enhances the IT infrastructure (products) and organization (people, process) security, and provides sound financial justification to the business for the expenditures required.

1. Gain (or grant) authority for the security review to proceed.

2. Define the scope of the review (IT service, location, application, etc.,) assign a team, and identify sources of information. Draft, review, and agree a project control document. You are now ready to start collecting data!

3. Begin stage 1 -- identify assets within the scope of the review (data, application/ software and physical assets.) A *Configuration Management Database* (CMDB) is valuable here, if you do not have a CMDB then ask around about important data, software or physical assets. You can leverage previous *Business Impact Analysis* (BIA) work that you have done here as well. *[See 'How to Win with BIA' DITY Vol. 2 #2 for more on BIA]*

4. Prepare a grid or table. A spreadsheet works well for this. (See figure 1.) For each asset, list the asset and the asset "owner" -- the owner is the person who knows best, the usage and value of this asset. This process also raises the level of acceptance of your review findings and proposals.

5. Interview the asset owner; have the asset owner value data and software assets by the impact/cost resulting from loss of Confidentiality, Integrity, or Availability; and physical assets by replacement cost. Have data owners consider the impact of the following attributes of their asset:
   a. Confidentiality -- impact of or sensitivity to disclosure of the asset to non-authorized parties, e.g., "employees," "contractors," etc. Use confidentiality requirement categories of **public** (0), **restricted** (1-5), **confidential** (6-9), and **secure** (10).
   b. Integrity -- impact of unknown or unauthorized modification e.g. "data input errors," etc. Use integrity requirement categories of **low** (1-3), **moderate** (4-7), **high** (8-9), and **very high** (10).
   c. Availability -- impact of the asset being unavailable for various time frames, e.g., "less than 15 minutes", "1 hour", "1 day", etc. Use availability requirement categories of **low** (1-3), **moderate** [OK to recover in days] (4-6), **high** [hours] (7-8), **very high** [minutes] (9), and **mandatory** [cannot be down] (10).

   For a, and c above, have the data owner first choose a category for each, then a value within the category. For example, for Integrity, have them choose first from *low*, *moderate*, *high* and *very high*. Then, if they chose *moderate* in this case, ask them to rank the impact on a scale of 4 to 7.

   If there are existing measures already in place to control risks identify them during this stage. Update the grid and move to stage 2.

6. Begin stage 2 -- review and agree deliverables from Stage 1. Determine how likely each risk in stage 1 is by asking questions of support personnel, experts and other personnel using prepared questionnaires to try and asses the likelihood that the identified risks could actually occur. Consider Hackers (inside and outside the company), Viruses, Failures (hardware and software), Disasters (terrorism and natural), and People, process or procedure errors. Create a column for each threat. Use a categories of **none** (0), **low** (1-4), **moderate** (5-7), **high** (8-9), and **very high** (10). Update the spreadsheet for each asset.

7. Calculate the Risk entry by multiplying the Impact by the Vulnerability. Based on the risk score (impact X vulnerability) assign a label of **low** (1-33), **medium** (34-67), or **high** (68-100). Update the spreadsheet for each asset. You now have an agreed list of the most vulnerable areas! Since this list is developed with and agreed by the Business, you also have a powerful ally for justifying the need to proceed.

8. Begin stage 3 -- review and agree deliverables from Stage 2. Begin to identify and select countermeasures for those assets with the highest risk level. CRAMM contains a very large countermeasure library consisting of over 3000 detailed countermeasures organized into over 70 logical groupings. Of course, without the CRAMM software, you do not have this, but you can still come up with many possible countermeasures through brainstorming and researching the risks identified. *[See 'Availability Management on a Budget' DITY Vol. 1 #2 for more on using tools like CFIA, FTA,*

SOA and others to develop solutions.]

9. Consider countermeasures and ways to mitigate the threats. Focus on the higher-level threats first, but don't overlook quick, easy or cheap fixes to lower level threats. In Figure 1, notice that we also chose to implement some countermeasures for low level as well as high level threats. Give precedence to those countermeasures that:
   a. protect against several threats
   b. protect high risk assets
   c. apply where there are no countermeasures already in use
   d. are less expensive to implement
   e. are more effective at preventing or mitigating threats
   f. prevent threats rather than detecting or facilitating recovery
   g. can be implemented quickly, easily and inexpensively (even for low risk)

10. Raise an RFC for the highest-level threats; use your assessments as justification for the Change. Produce a schedule and plan for implementation of agreed countermeasure recommendations.

The concepts of CRAMM applied via formal methods like these ensure consistent identification of risks and countermeasures, and provides cost justification for the countermeasures proposed. Even without expensive CRAMM software, you can gain powerful benefits like driving Business/IT Alignment, bringing security risks to the forefront, and assisting in the cost justification of countermeasures.

--

- Subscribe to our newsletter and get new skills delivered right to your Inbox, click here.
- To browse back-issues of the DITY Newsletter, click here.

Entire Contents © 2006 itSM Solutions LLC. All Rights Reserved.