UNITED STATES NUCLEAR REGULATORY COMMISSION

NUREG/BR-0304
Volume 2, Number 2
September 2004

OIG Information Digest

Management and Internal Controls

Inside this issue:

Special points of interest:

- Are You a Safe Cyber Surfer?
- Spyware Problems
- Visa/Mastercard Scam

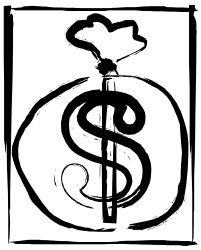
Management Controls: Business and Personal Needs

What are management controls? Are they for accountants and financial organizations only? Why do I need them? Why does NRC need them? Who needs management controls?

You may not realize it, but management controls are vital to almost all the important functions we carry out in our professional and personal lives. They help us to maintain order and control, and most importantly they protect us from harm and give us a measure of confidence that our business and personal activities meet our expectations.

What are management controls? The Office of Management and Budget defines management controls -- organizational structure and an organization's policies and procedures -- as tools to help program and financial managers achieve results and safeguard the integrity of their programs. On a personal level, management controls are tools to protect us from personal or financial harm. Management controls are the proverbial barn door that we want to close.

Are management controls for accountants and financial organizations only? Absolutely not! Many people think of management controls as something needed only to prevent financial harm to an organization. For example, a company needs controls over its assets to prevent employees from misappropriating them, and payroll controls to ensure that only bonafide employees or contractors receive payment. But, management controls also include a programmatic aspect. In other words, controls are needed to ensure that a program is functioning as management intends. Let's examine one or two NRC functions to see how management controls keep a program or activity on track.



NRC has many technical review processes for all areas of its regulatory activities. For example, one such activity is the review process for reactor technical specifications. To properly review any set of technical specifications, the agency needs a process (management

Management and Internal Controls (Cont. from page 1)

control) to ensure that the appropriate organizations review and approve the specifications. Another example of management control is the document concurrence process. This process is designed to ensure that all parties to a document concur on its content. From an investigative point of view, management controls or rules are enforced to ensure that no civil or criminal law is broken and there is no monetary loss to the Government. Every facet of NRC operations needs management controls.

Why does NRC need them? They serve to ensure the integrity and efficiency of the agency, protect the health and safety of the public, and prevent fraud, waste, and abuse within agency programs.

Why do I need them? In our personal lives, management controls could simply be referred to as controls. These controls safeguard and protect us. Let's look at a few examples.

Before we can set up an ATM account, we establish a password to prevent unauthorized persons from withdrawing money from our account. The password is the control. An alarm system for a home has a code to activate and deactivate the alarm. The code is the control. Imagine what could happen if we did not safeguard our passwords or alarm codes. In order to ensure that our checking account is not overdrawn, we should maintain a running balance. The running balance is the control. The financial consequences of overdrawing an account can be substantial.

Who needs management controls? Everyone and every organization needs management controls in one form or another. Even the most seemingly unlikely entities need controls.

In 1988, *TIME* magazine ran a story about how a Federal Bureau of Investigation agent infiltrated an organized crime family and was ultimately instrumental in gaining more than 100 Federal convictions of organized crime members. The article explained how the agent stayed undercover for several years, despite reservations from several criminal associates. According to the article, the director of the New York State Organized Crime Task Force stated, "The Mob, which once ran thorough security checks on any stranger, simply lacked the 'discipline and internal controls' to unmask the agent...."

Summary - Management controls bring order, discipline, and protection to organizations and individuals. On the business side, we use them to ensure that financial assets are protected and that programs are implemented as intended. On the personal side, controls protect us from personal and financial harm. Inadequate controls may ultimately spell disaster for any business or individual.

Audit Summaries

NRC's Personnel Security Program

OIG found that personal security program weaknesses pertaining to contractor access to NRC facilities could be placing the agency's information, facilities, and staff at risk. Specifically, program requirements were not consistently followed and the agency lacked a process for expeditiously resolving final access decisions for IT contractors with temporary access when issues arose in OPM background investigations. Program lapses occurred because managers had not effectively documented or communicated contractor security policies to NRC staff expected to carry out these policies. As a result, some contractors were inappropriately given access to NRC facilities and data, potentially jeopardizing agency employees and information.

Management and Internal Controls (Cont. from page 2)

Computer Security Reviews

The security reviews found that the controls implemented by the regions are generally effective in reducing the risks associated with their operations. However, several areas needed improvement. These areas included administrative security controls, information technology controls, and physical security.

Management Controls Can Facilitate OIG Investigations

Management controls are a factor in virtually all OIG investigations – in some cases, this is because illegal or inappropriate activity is traceable through the review of official records, which are a form of management control. For example, OIG criminal investigators, in furtherance of their official duties, may review employees' Government-issued credit card bills to identify suspected inappropriate charges when suspicions about inappropriate use are brought to the attention of the OIG. Over the past 2 years, through such investigations, OIG identified six employees who used their Government-issued credit card for non-work related purchases. While most of these employees either paid for or intended to pay for these charges, personal use of the Government credit card is prohibited by NRC policy. In a like manner, cell phone and pager bills may also be reviewed for inappropriate use. Based on such information, OIG determined that an NRC employee incurred $43,000 in pager charges for usage not related to his official duties.

In other cases, individuals manipulate or undermine existing controls to try to hide illegal activities. For example, in 2001, OIG determined that NRC's parking garage contractor had stolen $1,713 in visitor parking fees from NRC by issuing two types of receipts to patrons. One type of receipt was legitimate; duplicates of these were kept to record customer payments owed to NRC. The other receipts, however, were not legitimate. These unofficial receipts were given to patrons, but copies were not maintained and payments recorded on them were not reported to NRC.

In a third scenario, prohibited behavior can occur despite the existence of management controls intended to prevent such activities. For example, although the agency uses software that restricts employee access to pornographic and other Web sites, OIG has substantiated that at least 11 employees have, over the past year, downloaded information from such sites onto their NRC computer. Thus, while it is likely that the software effectively prevents some individuals from accessing prohibited sites, it cannot entirely prevent such activity.

Computer Security

Are you a safe cybersurfer?

When using your computer at home to make a purchase online, do your banking, pay bills over the Internet, check in with your office by e-mail, or just surf the Web for fun, you open a gateway to the personal information on your computer, including credit card numbers, bank balances, and more. You may also be in for costly computer repairs and lost data, due to damaging computer viruses that can invade your computer through e-mail connections.

Fortunately, there are steps you can take to protect your personal computer, your information, and your peace of mind from computer hackers who try to slow down network operations or, worse yet, steal personal information to commit a crime. Here are some helpful tips from the security experts at the Federal Trade Commission (FTC).

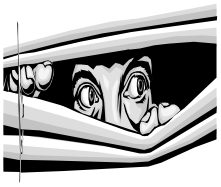
Computer Security

Some of these tips are well known by computer users, but they are always useful reminders.

- Make sure your passwords have both letters and numbers and are at least eight characters long.
- Install anti-virus software, particularly the kind that updates automatically.
- Prevent unauthorized access to your computer through firewall software or hardware especially if you are a high speed user. A properly configured firewall makes it tougher for hackers to locate your computers. Some firewalls block outgoing information as well as incoming files. That stops hackers from planting programs called spyware that cause your computer to send out your personal information without your approval.
- Don't open a file attached to an e-mail unless you are expecting it or know what it contains.
- Never forward any e-mail warning about a new virus. It may be a hoax and could be used to spread a virus.

Spyware or adware...are they the same?

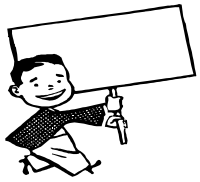
Have you noticed, while you are surfing the Internet or as you log onto a certain Web site, creative little banners or characters jump across your screen telling you you've won a prize? Or, they might suggest that to make your program run faster you should click on this button? Well, don't be fooled by these cute little advertisements because they just may be what are called spyware or adware.



Spyware is software that aids in gathering information about a person or organization without their knowledge and consent and which may send that information to another entity. It has reportedly caused 50 percent of all crashes on computers using Microsoft systems. Spyware can also assert control over a computer without the user's knowledge. There are many "click-on" download tricks that spyware programs use to sneak onto computers, unbeknown to the user. It is commonly installed on your PC as a hidden addition to a legitimate program, by visiting Web sites, or through spam e-mail. For example, some spyware programs use deceptive pop-up windows so that if a user clicks on the "Close Window" button, that click counts as consent for the software to be installed.

Adware is any software application in which advertising banners are displayed while a program is running. The authors of these applications include an additional code that delivers the ads, which can be viewed through pop-up windows or through a bar that appears on a computer screen.

Spyware and adware quietly and secretly capture everything you do online. Unlike the instant impact of a virus, spyware and adware programs never reveal their presence on your personal computer.



Spyware can seriously interfere with your computer operations and compromise your privacy. Spyware makes your computer's performance and Internet access slow to a crawl. Serious infections can lead to a corrupt hard drive and exposure of private information, user names, and passwords, or, at worst, identity theft. Pop-up ad problems, a different homepage that you can't change, and a slower PC, may be indications of a spyware problem.

A cookie, is a piece of information sent by a Web server to a Web browser that the browser is expected to save and send back to the Web server

Computer Security (Cont. from page 4)

whenever the browser makes additional requests of the Web server. Cookies are another means of tracking your surfing habits and can be used by spyware to gather more information about you. Delete your cookies on a regular basis and never open unsolicited e-mail. If you do not know who an e-mail is from, delete it. Other actions consumers can take:

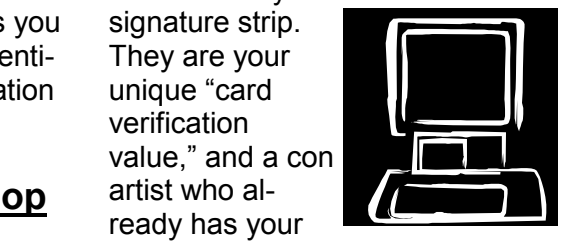
- Implement new security upgrades made available by your Internet provider.
- Install anti-virus programs and update them regularly.
- Install anti-spyware programs to detect or block known spyware. Some spyware programs are free and can be downloaded from the Internet. Others are available at a nominal cost. Remember to update these on a regular basis.
- Be careful when browsing online and make sure you know exactly what a "free" program will do before downloading or installing it.
- If asked whether you want to install a program, make sure you know who's distributing it. Before clicking "yes," ask yourself whether you know enough about that company to trust them.
- Be wary of clicking on any pop-up ad even to close the window.
- Install an anti-spyware program, install a firewall, and ensure your virus protection is up-to-date.

By following these guidelines you should be safe from outside entities collecting private information about you.

When VISA's Good Cop is a Bad Egg.

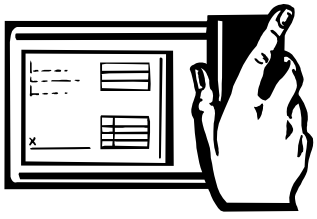
A call from "Security" can trick you into revealing what you shouldn't.

You receive a telephone call from a person claiming to be from the Security and Fraud Department at one of the major credit card companies stating that your card has been flagged for an unusual purchase pattern. They ask, "Did you purchase six Dell computers at three different locations in your area for $3,197.23 each?" "No," you answer without hesitation. "Then we will issue you a credit," the caller says. "To verify that you're in possession of your card, please read off the last three numbers that appear on the back." You are more than happy to agree. The caller gives you a confirmation number and encourages you to telephone with any questions you may have and then hangs up. He never asks for your card number–he asks for very little–so the word "fraud" doesn't enter your mind until you get your statement and find it filled with charges you don't recognize.



Where did you go wrong? By giving away those three little numbers on your signature strip. They are your unique "card verification value," and a con artist who already has your card number can use them to convince online and phone merchants that he actually has your card and hasn't just ripped off your number.

Officials at VISA and MasterCard are well aware of the scam, which seems to have blossomed this past spring. The giveaway is that the caller is asking for personal data. If you ever get such a request, explain that you don't discuss your credit card over the phone and say you'll call back. If the caller is legitmate, he'll understand. Then dial the 800 number on your card to see if his story checks out.



United States Nuclear Regulatory Commission

Office of the Inspector General
Mail Stop T5D-28
11545 Rockville Pike
Mail Stop T 5D28
Rockville, MD 20852

Phone: 301-415-5930
Fax: 301-415-5091
Hotline: 800-233-3497

We're on the Web!! Log onto the NRC Website and click on the links to the Inspector General Hotline!

TDD now available at the Office of the Inspector General. For any complaints of fraud, waste or abuse please dial 1-800-207-2787.