

# Canaudit Perspective

November 2003  
Volume 4, Issue 11

## Points of Interest:

- The waiver system is often abused
- Waiver requests
- The real solution
- IT Audit & Security Boot Camp
- Gordon's Books

## Security Waivers: The exceptions that can lead to disaster



Security officers are constantly identifying risks and taking steps to mitigate them in their quest to identify and eliminate security issues. One of the cornerstones of a protected network is strong policy, approved at the executive level and enforced by management. In many cases, legacy software or certain hardware technologies cannot conform to these policies. To facilitate the implementation of controls, while permitting some exceptions, management often implements a waiver system. Items that cannot meet the security or administrative policy are reviewed and granted an exemption, or waiver, for a period of time.

**The waiver system is often abused**, resulting in significant control issues. I strongly believe that the waiver system is used to provide legitimacy to flagrant policy violations that pose a significant threat to corporate security. Waivers increase the likelihood of fraud and malfeasance and perpetuate an unhealthy attitude towards control. Simply get a waiver if you can't comply with a control.

The waiver system is intended to enable management to grant temporary relief from a policy in specific instances when compliance is not possible. With the approved waiver in place, the vendors and staff have an opportunity to correct the issue and implement a safe and sane control solution. The waiver system also enables the early implementation of a policy that enhances controls. Even I believe that partial implementation is better than no implementation.

Waivers should not be granted every time there is an exception. Normally there is a committee that reviews the issues to determine if the problem truly cannot be fixed and that a waiver is justified. This committee may be composed of the CIO, senior IT management and senior members of the user community. This committee, in my mind, is not independent. They may want to sweep the policy violations under the carpet, defer problem resolution and, as a result, perpetuate control weaknesses. It is easier to approve a waiver than it is to fix the problem. I understand their position. Some legacy systems have inherent control weaknesses. It is expensive and labor intensive to replace this software with a new product.

Generally, waivers are granted for a three to six month period. Most of the waiver policies I reviewed permitted extensions, usually for a period not exceeding a year. Waivers cannot be renewed beyond the limitation period. I often find that waivers are frequently extended beyond the waiver limitation as no one is

enforcing the waiver policy. I have never encountered an organization that regularly audits waivers to ensure compliance and to identify items that fail to meet the required conditions for a waiver or items that exceed the time limitation.

Another concern that I have is that waivers may be granted even though compliance is possible. Sometimes funding issues causes this. In other cases, there may be a skills shortfall that prevents the organization from properly implementing the required control. Most often, I find that management does not want to resolve the issue. These attitudinal waivers cause me great concern. Compliance is achievable, yet for whatever reason, the waiver is perceived to be the optimum solution in the minds of the business managers.

If your organization chooses to use a waiver system, then there must be strong controls in place to ensure that waivers are only granted when justified, after a stringent and independent review process. The reason for the waiver must be clearly documented. The cost of remediation and the budget approval for the remediation effort should also be included with the waiver request. Any risks related to non-compliance should also be documented to ensure that management is aware of the business risk that they are accepting during the waiver period.

**Waiver requests** are often a result of operational issues. For example, I often see waivers on database exports or backups. When an application is implemented, there is usually no problem performing the required exports and backups. As time passes, the databases grow and nightly batch processing may expand to the point where the backups cannot be completed before the start of the next business day. Rather than addressing the performance issue, a waiver is granted that permits an incremental export or backup. Over time, database growth causes the timeframe for incremental export to exceed the time available. When this occurs, a waiver is granted so that the incremental export or backup is performed twice a week or on weekends.

**The real solution** would be to find the cause of the performance degradation. This is normally insufficient physical memory causing unnecessary overhead, underpowered hardware, poorly structured database indices or inefficient SQL or SQR programs. Finding and fixing these issues requires a very good DBA and performance tuning tools or utilities. It is easier to get the waiver than fix the problem. Easier that is, until disaster strikes! Days or even weeks worth of data could be lost if the database cannot be properly recovered.

I also find waivers used when passwords cannot be changed. Some of the common excuses I hear are that the vendor or contractor require a standard password so that they can perform emergency maintenance. If a standard password is used, you can be sure that hackers will learn of this quickly, enabling the hacker to easily compromise your system. I have also seen password waivers used for database access accounts. PeopleSoft and other such applications use these accounts to access the Oracle database. These passwords are often created during application development when there are many contractors who "must have the password" to build and test their modifications. When the application goes into production, the password is not changed. Furthermore, because of the "large number of SQL and SQR programs with embedded passwords," the password cannot be changed. A waiver is granted, and the application is highly exposed to unauthorized access and update by the large number of people who know the password. If the SQL and SQR passwords are poorly secured, then the application is also highly exposed should a hacker or disgruntled employee gain access to the password that is stored within these programs in clear text.

Sometimes our clients grant modem waivers to enable the administrators to bypass the VPN or firewall to perform emergency maintenance should the firewall or ISP fail. These modems do not have secondary authentication in place. When we suggest that the modem be restricted or controlled using secondary

authentication or biometrics, we are told that there is a waiver in place and the client is permitted to keep the modem. This is foolhardy to say the least.

We occasionally find waivers granted so that machines do not have to be patched. This is normally due to vendor software products that will not work if patches are installed. Rather than force the vendor to correct the issue, the waiver grants them an exception. As a result, the machine is exposed to a security or performance issue that can seriously interrupt processing or permit the system to be compromised by hackers, contractors or disgruntled employees.

Many of the above items can cause serious issues with the Sarbanes-Oxley Act of 2002, a public company accounting reform and investor protection act. Within this act there are specific requirements for disclosing information technology risks. Some of the risks, for which waivers have been granted, will need to be disclosed or the organization may face penalties or even criminal charges for non-disclosure. All waivers need to be reviewed on a regular basis to determine if there are Sarbanes-Oxley issues. Wise auditors and security officers will use the disclosure requirements to discourage the renewal of existing waivers and prevent the issuance of new waivers that cause Sarbanes-Oxley disclosures.

Waiver tracking is also very important. Often management does not know the cumulative risk of outstanding waivers. A summary of each waiver and the specific risks should be provided to management. I believe that management will quake in their boots when they understand the cumulative risk of outstanding waiver issues.

Another good practice is to perform a periodic impact analysis of the highest risk items. Management needs to know the business impact should the risk underlying the waivers occur. Keep in mind that the waiver system documents known risks and management's acceptance of those risks. As a result, the waiver system and specific waivers could be used against the organization should there be civil litigation. Damages could be trebled if the organization is deemed to be negligent. Legal negligence may occur if management had prior knowledge of an issue, that the occurrence of the issue has a significant cost, and that management chose to accept the risk when a prudent person would not accept that same risk. Imagine how foolish a company would look in court if a plaintiff was able to prove that management had a policy to patch machines and that a waiver was obtained to enable noncompliance to the policy. A company machine is then infected with a worm or virus and attacks other companies, creating a costly Information Armageddon. Victims of the forwarded virus or worm could sue the company in a heartbeat and likely win. In addition to the costs of defending the case, the damages, and penalties, this would be a significant public relations nightmare.

Management should also be notified on a quarterly basis of all permanent waivers and any waivers which have been renewed two or more times. Extensions, while intended to provide a little more time to achieve compliance, are often abused. Ensure that management receives periodic reporting of the expiry dates of critical waivers. This enables management to encourage staff to remedy the issue, eliminating the need for further waivers.

The waiver review process is much easier if there is a waiver database. This should document the reason for the waiver, the expiry date, the risk level, and business impact if a control breakdown occurs. The budget for the remediation and the percentage of completion should also be tracked in this database. Lastly, management should ensure that the appropriate staff is assigned for the task of remediation and that it occurs on a timely basis. If your existing staff cannot implement the required remediation, then hire someone who can.

As you can see, I feel very strongly about waivers. I believe that they are occasionally required, provided there is a concerted effort to bring the issue into compliance. Also, management must actively support the remediation efforts. Waivers that extend beyond a year can greatly increase business risk and expose the organization to excessive costs or a public relations disaster should a control violation occur. I strongly suggest that a full waiver system audit be performed annually as part of the general controls review. If your audit or security groups are unable or politically uncomfortable performing this review, Canaudit would be pleased to conduct the waiver audit. I love these audits and look forward to the issues that we will identify.

[Register](#) for our 5-day, hands on IT Audit & Security Boot Camp  
Fairfax, VA – December 1-5, 2003  
Instructor: Gordon Smith

For more information please contact Jennifer Hoffman at 805-583-3723 or [jennifer@canaudit.com](mailto:jennifer@canaudit.com)

As always, the opinions in this article are mine and mine alone. Please send any comments you may have to [gordon@canaudit.com](mailto:gordon@canaudit.com). I look forward to receiving your input on this important issue.



Mr. Smith is listed in the WHO'S WHO OF LEADING AMERICAN EXECUTIVES and has published 2 books titled [Network Auditing: A Control Assessment Approach](#) and [Control & Security of E-Commerce](#), both published by John Wiley and Sons.

Please feel free to forward this article to your co-workers.

A handwritten signature in black ink that reads 'Gordon Smith'.

Gordon Smith  
President, CEO