

University of Mississippi

eGrove

Newsletters

American Institute of Certified Public
Accountants (AICPA) Historical Collection

7-2007

InfoTech Update, Volume 16, Number 4, July/August 2007

American Institute of Certified Public Accountants. Information Technology Section

Follow this and additional works at: https://egrove.olemiss.edu/aicpa_news



Part of the [Accounting Commons](#)

Recommended Citation

American Institute of Certified Public Accountants. Information Technology Section, "InfoTech Update, Volume 16, Number 4, July/August 2007" (2007). *Newsletters*. 4036.

https://egrove.olemiss.edu/aicpa_news/4036

This Book is brought to you for free and open access by the American Institute of Certified Public Accountants (AICPA) Historical Collection at eGrove. It has been accepted for inclusion in Newsletters by an authorized administrator of eGrove. For more information, please contact egrove@olemiss.edu.

What's Inside

1 Trust and SuperUsers: Is Your Network Truly Safe?

Who is the SuperUser on your network? Does everyone with administrator access need it? These and other questions are addressed by Susan Bradley in an article that truly exposes the top layer of network security.

4 The Risk-Cost Retention Model: A New Approach to Records Retention

Putting paperless processes aside, how does a firm or company begin to evaluate how to retain records and e-mails that might be missed if they were deleted from systems and networks? Randolph Kahn, a speaker from TECH+, offers step-by-step techniques, including several "what-if" scenarios.

8 Donny Shimamoto, CPA.CITP An InfoTech Update Profile

9 Ebitz: Ensuring the Future of Your Applications

Nothing lasts forever. We know PCs come and go within a certain amount of time, as do your applications. What are the new rules?

Trust and SuperUsers: Is Your Network Truly Safe?

By Susan Bradley, CPA.CITP, MCP, GSEC

Susan E. Bradley, CPA.CITP, MCP, GSEC, is a principal with Tamiyasu, Smith, Horn and Braun in Fresno, Calif. Author of E-Bitz for InfoTech Update, Susan is an author, speaker and blogger at www.sbsdiva.com. She is the past chairman of the Technology Committee of the California Society of CPAs, and a writer on Windows and Patch issues for the *WindowsSecrets* newsletter.

In your network and in any network, there is a person who holds the keys to the kingdom. This person can get into any piece of software, application and database, which makes he or she the Supreme Being on the system with access to anything.

Do you know who this person is? Do you trust this person? This person can be an employee or outside vendor with whom you are entrusting all your secrets. Who is this person?

It's your network administrator – the "SuperUser" on the network who can be anywhere and gain access to everything. In large corporate IT environments, this SuperUser may be more than one person. In fact, there could be two people who put certain secrets together to obtain this role, but this User, above all users, is in every network.

On a stand-alone workstation, you can be the SuperUser. On a default installed Windows XP workstation, you are typically set up with administrative rights. You can log into anything, install any software you need and the system is entirely yours to do with what you wish. Because this is the default setting and the majority of us do not change this role, malware and spyware infiltrated our computers and networks. As a result, many badware authors know that we install systems exactly like this and code their malware accordingly.

Vista was released to begin the process of taking back these administrator rights from normal users. Through Vista, User Account Control (UAC) is designed to assist the possibly painful process of *not* running because administrator is easier on Vista. By design, programs run in lower-right levels, and when they request to run with Administrator rights, they offer the UAC prompt window for approval. For most newer programs, once the application is installed, you would never see this prompt again. It is only with the older software that there are still demands for administrator rights; you will see the UAC prompt over and over again.

Whether the administrator at the firm or the person installing the software is using the SuperUser for the Administrative rights account, the reality is that we all need to limit our use of Administrator rights on a network. As computer users, we don't protect the account enough. The bad guys trying to break in to our networks know that we are typically lax in our understanding and use of these key user roles.

If you looked at a typical network, you would see this occurring, with someone trying to break in or guess at the administrator's passwords. Typically, in even a small business network, you will see someone trying to authenticate on the email ports of port 25 in order to borrow the connection and send spam. You will see hackers attempt to guess the

InfoTech UPDATE

July/August 2007, Volume 16, No. 4. Publication and editorial office: AICPA, 220 Leigh Farm Road, Durham, NC 27707-8110. Copyright © 2007, American Institute of Certified Public Accountants, Inc. Opinions of authors and the AICPA staff are their own and do not necessarily reflect policies of the Institute or the Information Technology Section. Any hardware or software products mentioned do not in any way represent an endorsement by the Institute or Section.

All rights reserved. You may copy and distribute this document subject to the following conditions:

- (1) Copy all text without modification and include all pages.
- (2) All copies must contain the AICPA copyright notice and any other notices provided therein.
- (3) You may not distribute this document for profit.

Editorial Advisory Board

Roman H. Kepczyk, CPA.CITP, chair
InfoTech Partners North America, Inc.
Phoenix, Ariz.

Susan E. Bradley, CPA.CITP, MCP
Tamiyasu Smith Horn and Braun
Fresno, Calif.

David Cieslak, CPA.CITP, GSEC
Arxis Technology, Inc.
Simi Valley, Calif.

Chris Fraser, CPA*.CITP, MCP, MBA
Sunera LLC, Tampa, Fla.

Michael W. Hamish, CPA.CITP
Fios, Inc., Portland, Ore.

Michael S. Kridel, CPA*.CITP, CFC
Daszkel Bolton LLP
Boca Raton, Fla.
*Regulated by the State of Florida

Mary MacBain, CPA.CITP
BKD, LLP
Kansas City, Mo.

Mark D. Mayberry, CPA.CITP
BDO Seidman, New York N.Y.

Anne Stanton, CRM-MVP, MBA/ACC
The Norwich Group, Norwich, Vt.

Nancy Cohen, CPA.CITP, executive editor,
AICPA

Scott H. Cytron, ABC, editor
scytron@sbcglobal.net

If you wish to change your e-mail address or update your member profile, please send an e-mail to service@aicpa.org.

For questions about your subscription to InfoTech Update or other questions about your IT Membership Section benefits, please contact the AICPA at infotech@aicpa.org or leave us a voice mail message at (888) 777-7077 (Option 4).

passwords for Admin, Administrator or other typical Administrator-named accounts.

They, among others, know that these accounts are the "gold mine" of the network. As a result, this is why one of the first servers or even the workstation hardening techniques is to change the true "Administrator" account to be named something else. This built-in master account is sometimes called the "500" account in honor of its Security identifier in the Microsoft system.

This 500 account is the system administrator account, and as noted, it has full control over the system. While protecting this account through the means of good passwords is a must, depending on the risks of the network, using two-factor authentication should seriously be considered.

If your administrator password is 1234, qwerty or Admin, you need to seriously question how much you value your network. Passwords will continue to be a valuable defense mechanism, but many companies don't sit down with their users and explain the reasons for password policies. If you have a hard time guessing a password, it buys the network administrator time to watch the event logs, making it easier to see someone or something trying to break in. With longer and stronger passwords, time goes by faster. As a result, no one is able to break in.

The key is understanding the importance of the data in which you are protecting. As accountants, one can only imagine the critical pieces of information we regularly take for granted on our networks. From Social Security numbers in tax preparation software databases, to credit card account numbers and other key critical information, we all need to understand that even in small peer-to-peer networks, the accounting data inside a computer system has some very private information that must be protected.

As a result, a user account with administrator rights should be eliminated or significantly restricted, with additional authentication techniques applied to ensure the

accountability of who obtained access during the use of this account. Separate logins for each person needing administrator access should be set up to ensure there is no one SuperUser account, but, in fact, traceable accounts whose access is logged and accounted for.

Consider only giving those users the minimum access they need to perform their role. For example, if all they are doing is managing e-mail accounts, they have no need to have an account with SuperUser rights. If all they are doing is adding users, again, you can set up levels of access so that the Power user only has the bare minimum rights needed for access. Software vendors typically publish documentation that clearly identifies the bare minimum permissions needed to deploy and manage the software. As much as you can, your firm should strive for this bare minimum level when giving employees their duties and roles on the firm's network.

Even with the use of good, strong passwords, you may still want to have strong two-factor authentication, especially on SuperUser accounts. Think in terms of a safety deposit box at the bank, where you place your most valued items. They are protected by your key and the bank's key. The use of two-factor authentication in a token is similar. Until now, only medium and large businesses could afford such two factor technology, but recently, several vendors have stepped up to the plate in this additional authentication technique.

One vendor, Scorpion Software, even designed a two-factor authentication solution that fits with a certain remote access technology native to the current version of Microsoft Small Business Server 2003, and will even be included in Windows Home Server. Using a token to generate a one-time password that's unique to that time session, the user can enter in his or her username and password, followed by the token value for an additional authentication technique.

Value-added resellers and providers are deploying Scorpion's AuthAnvil to better track the remote access to a server by their

employees, and will be able to quickly and easily remove access – if an employee’s access needs to be revoked. The token that they use can be easily and quickly revoked without impacting the working server. The two-factor authentication software also can be used in other Windows applications, as well as to set up custom two-factor authentication needs by vendors as well. Thus, in the case of the value-added reseller, the use of two factor tokens is giving additional accountability and traceability of each consultant’s access to that network.

The use of the SuperUser account comes with great responsibility. At times, that responsibility could mean a risk of trust. Several years ago, one of the security experts at Microsoft was surprised to get questions on how a firm could take back some rights and the trust of Administrators. Microsoft’s [article](#) on this topic was quite clear. Administrators must be trusted, and if they are not, then you must assign them the traditional pink slip and remove them from your organization.

If you do not trust the person on your domain to be inside your payroll data, your client data or anything else on your network, you need to seriously fire that person. Even when hiring someone for this role, you should not consider this person to be merely cheap IT personnel, but someone able to get inside of everything on your network. Background checks may be needed or required in certain industries, and in general, are strongly recommended. The SuperUser is indeed just that – a person who has the ability to obtain access into all of the information on a network.

In fairness, you can set up encryption or other methodologies to protect the data, even from the SuperUser account. However, even with this additional protection, that SuperUser has the great ability to damage a network and its data, possibly leading to the firm’s ultimate damage and demise.

If you are a firm or business hiring outsourced IT personnel, ensure that the firms you hire have taken additional steps to ensure that your administrative usernames and passwords are kept securely, and additional steps are taken, as appropriate, to maintain the confidentiality of these passwords. Even for casual vendor access to a network, set up additional accounts to track vendor logging on and logging off, and disable the accounts once the project is done.

Even for my small home network, I keep an account for vendor access only. I reset the password each time I use it and disable it at the end of each session. Other vendors are beginning to use an “approve” method of vendor access, including Web-based remote access with approval on demand. They also see the risk of the use of usernames and passwords on a system as being too risky for them to have.

We have two issues facing us when it comes to the use of Administrator accounts. We first need to look at the use of this level of rights in our workstation, and then at the process of stopping the running of our systems in this manner. I set up the Web site of www.threatcode.com to help administrators identify soft-

ware that demands this right and devises ways around that issue.

Second, when setting up these accounts in our domains and networks, we need to clearly and carefully monitor who has access to these accounts. Consider using two-factor authentication to ensure additional accountability, along with the audit ability of access. Revoke and close accounts when employees leave and question their need to have SuperUser accounts. Because administrative rights are powerful weapons, it is best to place them in a limited number of hands.

.....
Contact Susan Bradley at sbradcpa@pacbell.net ●

“ **If you do not trust the person on your domain to be inside your payroll data, your client data or anything else on your network, you need to seriously fire that person.** ”



The Risk-Cost Retention Model: A New Approach to Records Retention

By *Randolph A. Kahn, Esq.*

Randolph A. Kahn, Esq., is owner of Kahn Consulting, Inc., a consulting firm specializing in the legal, compliance and policy issues of information management and information technology. A speaker at AICPA's TECH+ Conference, he is a two-time recipient of the Britt Literary award, the author of dozens of publications and co-author of *E-mail Rules*, *Information Nation*, *Information Nation Warrior* and *Privacy Nation*.

Records retention is broken. In the past, this might not have been so serious, but today, records and information management (RIM) matters. Today, the proper application of retention rules to a vast array of business content is more important than ever. Most business information is in electronic form, distributed across more IT infrastructures, facilities, and geographies than ever before. More people, from employees to IT staff members, create, receive and have control of records, making every employee with a computer a de facto records manager. However, for many employees, following the proper retention rules – if they even exist – is not a top priority.

Can You Agree on These Retention Assumptions?

Agreeing with the IT, legal and business departments on these issues will help organizations determine a functional records retention model.

- Storing information without a business or legal need is not a good use of resources.
- The majority of business records are born digital.
- Laws require retention of some information, including e-records.
- Every organization has some retention responsibility.
- An organization can't keep everything forever.
- An organization can't get rid of everything tomorrow.
- There are business costs and legal risks associated with storage decisions.
- Storage and retention are different activities.
- The volume of records is growing exponentially.

Employees are unlikely to go through each e-mail, spreadsheet or word processing document to evaluate, code and manage it if it requires reviewing a list of hundreds of retention categories to determine the appropriate retention period. If employees are going to get records retention right, it is better to be fast, easy and intuitive. The key is to develop a records retention model that is

“**Creating a new approach to retention requires input and buy-in from the IT department, the legal department and business executives, at a minimum.**”

user-friendly, simple, seamless and easily applied. Unfortunately, organizations all too often don't have an adequate way to ensure that records are being properly retained. However, developing an effective records retention model isn't impossible. Reengineering the development of retention rules can make this task simpler and, therefore, more likely to be successful.

Build the Evaluation Team and Evaluation Methods

Creating a new approach to retention requires input and buy-in from the IT department, the legal department and business executives, at a minimum. There are numerous interrelated issues that need input from a variety of different perspectives to make sure the new retention plan works for the enterprise overall. Assembling the right team is tantamount to success and to getting buy-in from the rest of the organization. After assembling the right team, begin evaluating the various retention options for the organization. Gather ideas from colleagues about what may work and develop a list of suggested approaches. That list may look something like the following one, and even though some of these ideas may not seem feasible – and, in fact, might not typically be considered by the RIM community at all – those tasked with solving the retention problem should expect to find advocates of each of these approaches within their organization. Some possible retention options include the following:

1. Get rid of everything immediately.
2. Keep everything forever.

3. Set the retention periods by record type for the employees to apply with some RIM help (the traditional approach).
4. Use software to automatically apply retention codes and make decisions about what is a record.
5. Capture a copy of everything on the backup system.
6. Base retention on a fixed period that is long enough to address event-based retention and long retention requirements.
7. Base retention on the business function (one retention category for everything deemed to be a record in a particular business unit) and provide a way of dealing with exceptions.
8. Base retention on the business function with current retention synthesized into fewer, higher-level categories, organizing them in a way that gives users fewer choices and still makes it legally consistent.

Determine the Best Approach

Getting substantive input from colleagues representing various business units will help build consensus and lead to the best retention solution. For example, lawyers are likely to have different concerns than IT executives, who, in turn, are likely to have different concerns than e-mail server administrators. It is important to determine how the chosen retention option will affect the organization's user needs, business needs, access requirements, legal requirements and litigation environment. The following risk-cost retention model can be used to help focus the retention discussion on the right set of issues and determine the best approach for the organization.

Using the Model

As a team, discuss each option's costs and the risks for each of the issues listed below, and how they're related to the organization's business, technical, legal and records management perspectives. Using a scale of 1 to 10, with 1 representing the lowest cost and lowest risk, assign a numeric value to represent the cost and risk in each of the four areas for each of the options listed. Then, total the numbers. The higher the overall score, the less attractive this approach will likely be for the organization. The model could be customized to add analysis to the other issues (e.g., benefits) or weight to those issues that are of greatest importance (e.g., complying with laws). The focus of this exercise should be to identify the trade-offs each approach will require.

Discussing the Various Approaches to Retention

Option 1: Get rid of everything immediately.

If an organization got rid of everything shortly after its creation, the cost of management would be low, but the risk of not having something that was needed would be high. Risk of system failure would go down because the stuff clogging systems would be

purged. There are benefits to this approach, but it may also create risk and legal exposure that are not acceptable. Not being able to produce information for lawsuits or regulators, or failing to retain records in conformity with laws, would create exposure that well-run organizations will not find acceptable.

Option 2: Retain everything forever.

The risks and costs associated with keeping everything forever may be high. One of the perceived benefits of keeping everything is that it alleviates concerns about not being able to produce something in response to a lawsuit. Yet, when considering the resulting difficulty of finding and retrieving a specific item across the enterprise, it is obvious that this could not be done economically and expeditiously. Furthermore, the risk of system failures and costs associated with management would be very high, making this option not as attractive as others.

Option 3: Apply retention by records type with RIM support.

Those representing business units, other than records management, may be concerned that because of the sheer volume of records, coupled with the large number and complexity of retention rules, this approach requires too much employee time to code all content correctly. Business executives may see this task as something that they do not want employees spending much time on because it does not add positively to the bottom line. Another common perception is that employees will always find a way around such processes.

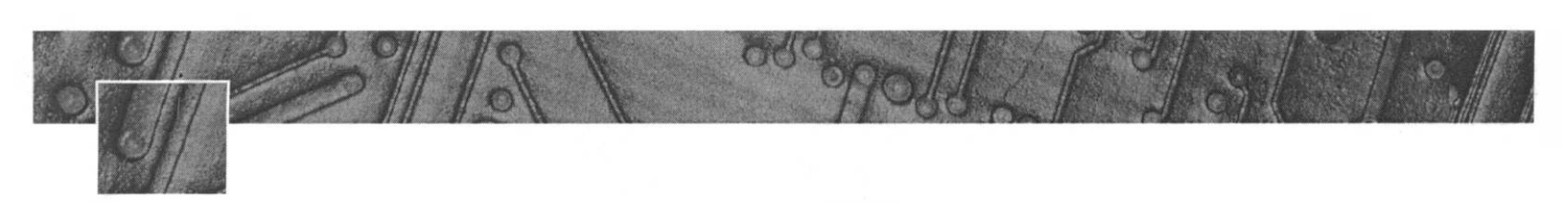
Option 4: Use software to automatically apply retention.

Auto-classification, or artificial intelligence software that can "learn" to get retention right over time, would require virtually no employee's time and may be very attractive at first blush. Once it is coded, record destruction also would be automatic. However, a lawyer may be concerned about allowing technology to code and manage company records, knowing that the software will fail a



Auto-classification, or artificial intelligence software that can "learn" to get retention right over time, would require virtually no employee's time and may be very attractive at first blush.





significant percentage of the time. While IT may point out that the technology will make fewer mistakes than employees do, the lawyer will likely point out the difficulty of explaining to a judge why the company's records policies are not properly applied a large percentage of the time and why it may have allowed a computer to mistakenly – or illegally – destroy evidence. IT responds that even if the organization *doesn't* completely rely on such technology, it could be used to help reduce the problem.

Option 5: Capture a copy of everything on the backup system. Someone from the disaster recovery team may suggest capturing a copy of everything on the backup system and storing it all for a set period of time. This approach consists of issues involving inaccessibility and difficulty in retrieving needed records to respond to business needs, litigation discovery requests, requests from regulators and other legal requirements. The hard costs of capturing a copy of everything is higher than needed because many non-records also will be saved. Lawyers and records managers may assert that the approach would probably violate the law if records that need to be retained longer are disposed of, according to the disaster recovery tape recycle schedule. Records managers would also point out that the disaster recovery system does not provide sufficient RIM functionality.

Option 6: Base retention on a fixed period of time. Instead of capturing a copy of everything on a backup system, records could be retained wherever they are located, but for a fixed period of time. The discussion around this may be the same as option 5. In the end, the organization would store a great deal of non-record material without any real benefit. Furthermore, significant costs would be incurred for storing and managing this mass of content – particularly when some records would end up being stored and managed on systems that were never designed to deal with the volumes or controls that might be required. Unless the retention was very long, invariably, records requiring retention would not be retained in accordance with laws. In addition, this approach does not provide a satisfactory means to deal with event-based retention of records.

Option 7: Base retention on business function (one retention category for every record in a particular business unit) and provide a way to deal with exceptions. IT might suggest keeping all e-mail for a set period of time based on the business function of the group. For example, accounting would keep everything for seven years, human resources would keep everything for 10 years and so on. While it may seem easy, it might be *too* simple because this approach fails to recognize the different kinds of content in each business unit or address records that are subject to event-based retention. In such a situation, the exceptions list would likely be sizable.

Option 8: Base retention on business function, synthesizing retention into fewer higher-level categories that give users fewer, but legally consistent, choices. This variation may make the most sense to the team. Working together, RIM, IT and legal staff coalesce categories of records that

have the same retention periods and create higher-level “buckets,” into which users can drag and drop records. Although this requires more work up front, it accommodates a number of the issues. And, although this gives responsibility to employees, having fewer choices makes selection faster and more likely to be done properly.

Keep Options Open

Using this risk-cost retention model takes a team approach from legal, business, IT and RIM, allowing all perspectives and options to be considered. It also provides an objective basis for discussing the hard issues around retention and choosing a retention approach that best meets the needs of the organization. With the proliferation of records – electronic and paper – in today's business environment, it is imperative to choose an approach that makes retention decisions and applications easy for every employee. As the organization's needs change and technology evolves, use the model to consider new or improved approaches with an aim to simplify, simplify, simplify, and then simplify some more.

Applying the Risk-Cost Retention Model on a Flooded E-mail System

How would the risk-cost retention model work when applied to a real situation? Consider the following example:

The CIO of a manufacturing company that employs 10,000 people at locations worldwide is faced with serious e-mail system functionality issues. The company has experienced an exponential growth in the volume of e-mail clogging the company's systems. Growing numbers of electronic discovery requests have taken IT staff away from their real jobs, often for days at a time. Thus, the CIO imposes several policy “fixes” to address the over-burdened e-mail system.

First, the CIO cuts mailbox sizes, limiting what employees can store. However, after dealing with minor employee revolts and executives who are not fully on board, the CIO is forced to accept that limiting mailbox size has not really addressed any of the core problems.

So, the IT department issues another directive, requiring employees to store e-mail on their local computer in personal (.pst) files or on removable disks rather than on the server. However, lawyers intervene, making clear that .pst files only make discovery more burdensome. So, reluctantly, the CIO capitulates.

When the directive is circulated, it indicates that the IT department is planning to purge the content of the entire e-mail system every 90 days, without regard to its contents. Regarding the records manager's concerns that were expressed to the legal department, a meeting is called by the CIO to develop a better, more holistic approach that deals with the importance of records retention, litigation preservation requirements and IT systems functionality limitations.

Gathering Input From Stakeholders

A meeting occurs, which consists of representatives of various business units with an interest and a stake in decisions surrounding e-mail retention. The following shows some of the arguments for various retention approaches stakeholders might make in such a situation:

The CIO starts off by saying that the "get rid of everything immediately" approach to retention should be considered. After all, "E-mail is not a record and is not needed," the CIO says, "so don't waste resources any longer than necessary to store junk." The records manager is prepared with facts to move the group in a different direction, sharing data about industry use of e-mail for business purposes, and concluding by saying that while some e-mails are indeed junk, others are records and must be retained, according to the appropriate retention rules.

The company litigation head says that discovery certainly would be made easier and cheaper if there was no e-mail to look through. However, he asserts that as attractive as it may seem, cleaning house of everything tomorrow would violate recordkeeping laws, would likely destroy evidence needed for pending lawsuits, and would, in fact, destroy information that might be helpful to the company because it tells its side of the story in litigation. Therefore, he advises against such an approach. He reminds the group that the destruction of evidence provisions of the Sarbanes-Oxley Act of 2002 provides decades of prison time for the intentional destruction of certain information in certain situations.

Seeming not to hear the lawyer, the head e-mail administrator, who is responsible for mail servers, appears gleeful at the prospects that the current server failures and exponential growth in stored messages would be immediately resolved, and storage budgets would be freed up to use for other more "productive" IT needs. He makes clear that employees would really appreciate the improved system functionality by getting rid of everything after a short period of time. To himself, he admits that if he advocated this approach to "retention," he might lose a huge part of his storage budget to competing IT projects.

One of the business unit heads and a sponsor of the project notes that users would revolt because they "live and die" with e-mail. Therefore, this approach would never be supported by any of the other business executives. He notes that while it would be great *not* to see so much time and resources wasted, employees could not efficiently do their jobs without records, including e-mail records. The records manager reminds the group that the company already has a terrific retention schedule that should be applied to e-mail records. However, another member of the team interrupts, noting that employees will not take the time to do retention right, even if it requires lots of time searching through hundreds of retention schedule choices to find the right code for every e-mail record. The group goes on to discuss other options, but in the end, they just don't know how to come to a conclusion about the right approach to retention.

Applying the Risk-Cost Model and Making a Decision

The group turns to the risk-cost model for help. Collectively, the group determines that if all e-mail were destroyed after a short period of time, there would be a great likelihood that needed business information would not be available. They conclude that the "Risk to accessibility" of information is extremely high, so the group gives it a "10." In the next column, the group assesses the "Costs of information management and storage" (e.g., people, process, technology) and concludes that if everything were gone tomorrow, it would significantly reduce the costs associated with management; they assign it a "1." The group then goes through the remaining technical, legal and records management risks, and costs for this option, and the remaining even options. The total score column indicates that for this company, keeping everything forever with 71 points has the greatest risk and cost so that it would be the least desired option. Basing retention on business function and synthesizing retention into fewer higher-level categories, the group scored 24 points with the lowest risk and cost for this company.

.....
**Contact Randolph Kahn at
rkahn@kahnconsultinginc.com**

This article first appeared in *The Information Management Journal*, vol. 40, no. 3. ©2006 [ARMA International](http://www.arma-international.com).
Reprinted with permission. ●

INFOTECH UPDATE PROFILE

Donny Shimamoto, CPA.CITP

Donny Shimamoto, CPA.CITP, is founder of IntrapriseTechKnowlogies, a Hawaii-based business providing executive-level technology management, enterprise architecture, business performance management, information architecture and management, technology risk management, and knowledge management consulting services.

Donny chairs the Technology Advocacy Committee of the Hawaii Society of CPAs and is a member of the AICPA's IT Executive Committee. He was recognized as one of Hawaii's 2004 Top High Tech Leaders by the Pacific Technology Foundation and the Technology News Network.

We caught up with Donny from his office in Hawaii to find out more about his business, his views on accounting technology and a bit about how he uses the CITP to benefit his clients.

InfoTech Update: *Your Web site talks about "intraprise synergy." Explain what that is all about and how it benefits your clients.*

Donny Shimamoto: For us, the "intraprise" is the foundational structure of an organization. This includes accounting, information technology, human resources, the overlaying organizational structures, business processes and information necessary for achieving the organization's mission.

When an organization has good synergy, its core resources, finances/funding, technology, knowledge and people are all aligned in high performing organizational structures of, for example, teams and departments, who use integrated business processes without working in process stovepipes or vacuums. They all have access to the latest information and metrics about the organization's operations and business intelligence.

With "synergy," the benefit is clear—the right information gets to the right people at

the right time to make the most intelligent decisions possible in the context of a business process.

ITU: *As a CPA.CITP, what do you think qualifies you to do this kind of work?*

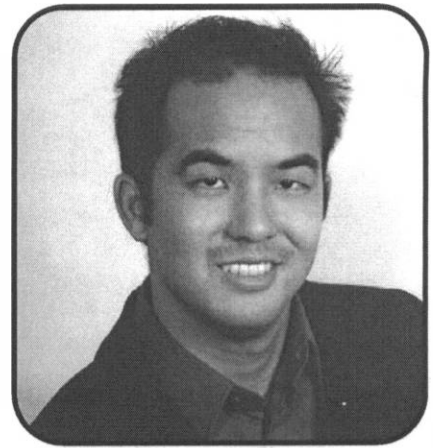
DS: My CPA distinguishes me as someone who has an understanding of how financial transactions and information flows throughout an organization, and what internal controls are necessary to mitigate the risks associated with those transactions and information. With the CITP, I've taken that base knowledge and added an understanding of what technology can and cannot do, how to actually design the data structures to capture the transactions, and how to build the systems that support the flow of information.

I help form a communication bridge as a translator between two very important groups within the organization; I can think and speak in both languages – accounting and IT. In addition, because I have worked in both areas, I have a keen understanding of what each group needs functionally, intellectually and emotionally, so both groups can stay focused to successfully complete a project. It is this ability to bridge the accounting and IT worlds that uniquely qualifies a CPA.CITP to do this kind of work.

ITU: *You are somewhat specialized in that you reside and work in Hawaii. Do you think there are any significant differences in technology consulting from your corner of the world versus somewhat who is in the continental United States?*

DS: The biggest difference is the size of organization. Hawaii doesn't have a lot of large corporations, so my biggest challenge is taking these "enterprise" concepts and scaling them down to work in a "middle market" environment.

In a smaller organization, the different business units work more closely together, so



**Donny Shimamoto,
CPA.CITP**

our projects tend to have a wider impact than something that is just being done for an isolated business unit. A disruption in one part of the business can have a much larger impact on the rest of the organization. To address this, I have to be a lot more focused on risk management and obtain a much higher level of trust from stakeholders across the organization before implementing changes.

ITU: *You obviously provide consulting services in a variety of technology arenas. If you had to name only one technology that all clients and prospects should implement, what would it be and why?*

DS: Business Performance Management (BPM) technology would be my recommendation. This technology has come a long way since its introduction several years ago when it just resembled spreadsheets on steroids. BPM technology now serves as a core part of any business intelligence strategy.

Many people think of BPM only as something for budgeting and financial reporting, but its use transcends accounting-focused implementations – normally called Corporate Performance Management – because these systems are also able to

handle any quantitative data related to any business driver. Rather than just working with dollar amounts, budgets and performance measurements can be based on business drivers and assumptions. These include, for example, expected number of units sold, number of billable hours, average contract close rates and average salary increases.

This technology also allows data to be captured at a low-level of detail and aggregated at each point of the organizational hierarchy, allowing complete transparency of the data down to the lowest level possible without having to go to disparate systems or a mess of spreadsheets. Executive dashboards and management reports are then all tied to the same base data so that there is "one version of the truth" – no matter what level the organization is at.

ITU: I know you were the first CPA.CITP in Hawaii, right? What do you gain from having the CITP credential and how do you feel it benefits your clients?

DS: The CITP credential has really helped distinguish me and put me into a class of my own state. It basically separates me from non-CITP CPAs who are very accounting focused and the IT professionals who are very technology focused. The unique blend of accounting and IT I bring to the table has enabled me to be recognized and selected for work, even when competing with national accounting firms or large IT consulting firms.

Most of my clients are CFOs or other CPAs, and my CPA.CITP provides them the reassurance that I will be able to understand their requirements (whether it be related to GAAP, internal controls or compliance). I also have the additional depth of experience in technology management to be able to advise them on technical issues and the risks associated with using technology in their organizations. ●

E - B I T Z

E-Bitz focuses on practical applications of various technologies to enhance a practice or business. Throughout 2007 Susan tackles 2007 Top Technology Initiatives' Honorable Mention list, numbers 11-15.

E-Bitz WITH SUSAN BRADLEY

Ensuring the Future of Your Applications

I have a phone that talks to my calendar and my computer that shares its information with the rest of the people in the office. I have a time and billing program that allows us to export names and addresses for mail merges. I have a tax preparation program that contains a database of clients, allowing me to go to a tax law database and determine which folk are impacted by new tax laws.

Sounds good, right? There's a problem. Because all three are using different database engines, it's not easy to migrate information seamlessly from one engine to another one without a mapping of the data or assistance from some third-party programs.

I have some workarounds to reuse data from one program to another. However, when you select a program, one of the hardest questions you should ask vendors is about their long-term plans for databases and applications' platforms. At one time, running a database as robust as Oracle was only for those who could

afford *expensive* software. These days, there are many variations of closed- and open-source database software that should be analyzed while you are making your decisions.

Question #1: Is the database back-end on something with a future?

A recent announcement was made regarding the future support of the Microsoft Foxpro database, a lightweight database engine I've seen in many different lines of business applications. Although it would continue supporting Foxpro, Microsoft decided to make this database more community-based; the latest version upgrade would be placed in a shared code space site. While there are many applications that work just fine without upgrades, the reality is that for many business decision makers, including myself, when I hear that a database is getting its last update, I begin to worry. I look to ensure that the vendor is planning

a path ahead. So when you get the answer to what database the prospective program is built on, check with the vendor to learn about future plans.

Question #2: Is the application preparing for 64-bit?

My guess is that everyone reading this article is using 32-bit machines on a daily basis. For most of us, the use of 64-bit processing and computing power is not yet in our reach due to the requirements of our applications. The advantage of the 64-bit platform is additional memory management and faster processing.

While you can run 32-bit apps on 64-bit operating systems, an issue arises when you start looking for drivers, printers and other items to attach to those workstations. At the present time, many of our applications and databases still work best on the 32-bit platform. However, most of your vendors should have announced or

be announcing their plans for 64-bit processing support.

What you should be doing at this time is ensuring that when you are ready to make the leap to 64-bit, your hardware will be ready. As a result, from now on, only specify 64-bit processors, knowing that you can install 32-bit software on any of these computers. When you are ready and your vendors are fully ready for 64-bit migration, you'll need to reinstall the software to support the 64-bit platform and reinstall your applications.

Question #3: Is the vendor looking to provide additional products or opportunities for interoperability?

In my own office, we have various databases we've built up over time in different platforms; the lack of true interoperability could be solved by ensuring we choose products from a vendor suite.

Many of the key platforms in the accounting industry are beginning to line up "suite" products that ensure you place your information into the database only once. In the case of industry applications, the push toward single sign on and identity management across multiple databases has given applications built for various industries a bit of a head start in this process. In fact, as many of these industry applications are built on various standard database platforms, it's usually relatively painless to find a database developer that can review the specifications of the platform to understand the needed data hooks.

Many of these platforms, from the smallest platforms to the largest, openly and freely publish the information about these data hooks. Whether you call this documentation API documentation from Microsoft or Source code from Open Source vendors, the result is the same. The vendors publish the necessary information to be able to call into the software and extract the needed information. At

times, the cottage industry that builds up around these add-ons and tools gets so large that an industry is built up around these needs. Some of the low-end samples include the vendors that sign up with the QuickBooks Developers network to the high end where many firms custom code and write software. These days, if a vendor won't provide this information, it's best to keep looking.

Question #4: Does your line of business application look like it was coded in 1984?

If you are still using a line of business application that you haven't updated since Spring 1984 – and you expect it to have the ability to talk to the calendar on your cell phone when cell phones didn't exist in 1984 – you might want to set your expectations for interoperability accordingly.

Computer programs, written back then, didn't have any of the types and kinds of data we regularly capture today. As a result, when you attempt to use old code to do the job of today's technology, you won't even have a mediocre experience. In recent years, the needs of applications and databases to have more interoperability has multiplied. Conversely, ensure that when selecting a newer database, you see a road map for change and growth as well.

Choosing a solution that has a clear application side versus a database side may future proof your project as well. It is likely that Microsoft's SQL Server, Sybase SqlAnywhere, MySQL, Oracle and other true databases will be able to be used and reused in the future. Whether your applications are on .NET, Silverlight, Ruby on Rails or Adobe Flash, the question if it will emerge as the dominant Web application platform has yet to be determined. However, the probability is high that the database can be reused, imported again and repurposed. Perhaps it's a language that we haven't even been used; yet, it will be the Web 2.0 application winner. So, while the data can be on robust,

stable platforms, on the application side, there's room for a bit more flexibility at this time.

Regardless of your size or whether you are a traditional CPA with a firm or working in business and industry, the rules for both are the same. When you shop for business applications, always ask what houses the data and what language the application is built on. Those two answers will tell you how future-proofed your vendor really is. Line of business vendors will always lag behind the bleeding edge, but if vendors are housing and building solutions on near-geriatric platforms that have no clue what interoperability is, it's time to reevaluate your systems.

Susan E. Bradley, CPA.CITP, MCP, GSEC, is a principal with Tamiyasu, Smith, Horn and Braun in Fresno, Calif. Contact her at sbradcpa@pacbell.net. Note that the opinions expressed here do not reflect an endorsement or recommendation from AICPA.

AICPA Top Technologies #13

Improved Application and Data Integration

Use of existing and evolving technologies to better integrate data between diverse applications allowing organizations to select and seamlessly integrate data and functionality between "best of breed" applications. Updating a field in one application automatically synchronizes that data with other applications.