Extreme Competition

Peter Fingar
Executive Partner
Greystone Group

pfingar@acm.org

Latest book:
Extreme Competition: Innovation and the Great 21st Century Business Reformation,
Meghan-Kiffer Press, 2006.
www.mkpress.com

EDP Audit and Control Redux

Over the past few years, as a result of my writing and speaking, I've sometimes been labeled as a visionary, as someone who evangelizes BPM at the 100,000-foot level. But, I confess, I've spent much of my career at ground level, sometimes even lower, programming SPS machine code in the 60s, then on to Assembler language, C++, and on to object-oriented component technology. So, it's a kind of relief to step away from the bits and bytes, and to relate increasingly advanced technologies to their *first principles* at the intersection of business and technology. What's kind of neat to observe is that the first principles change little, even as they get embedded in ever more sophisticated technology, whether it's going from paper journals to cash registers or from cash registers to point-of-sale systems. Each step change in technology represents a two-edged sword – more power and more loss exposures.

Recently, I've had conversations where the challenges of security, control, and auditability of multi-company, end-to-end business processes strike fear in the hearts of business executives. And well it should. Here's a snippet from an email dialogue with a government official related to BPM systems, "One concern I have in my brief scanning of the attachments is the apparent lack of concern for security. How to create ad-hoc work environments across company boundaries and still maintain the security posture of each company seems to be a glaring issue …." Let's use this email as a jumping off point.

Whether it's moving from a batch mainframe system to a distributed object system, or to a business process management system that spans multiple companies, the fundamentals of risk management still require addressing the same nine sources of loss exposure: Erroneous Record Keeping, Unacceptable Accounting, Business Interruption, Erroneous Management Decisions, Fraud and Embezzlement, Statutory Sanctions, Excessive Costs, Loss or Destruction of Assets, and Competitive Disadvantage. Of course, the kinds of internal controls needed to manage these loss exposures change with changes in the technology used to implement business systems. Let's turn back the clock to see how.

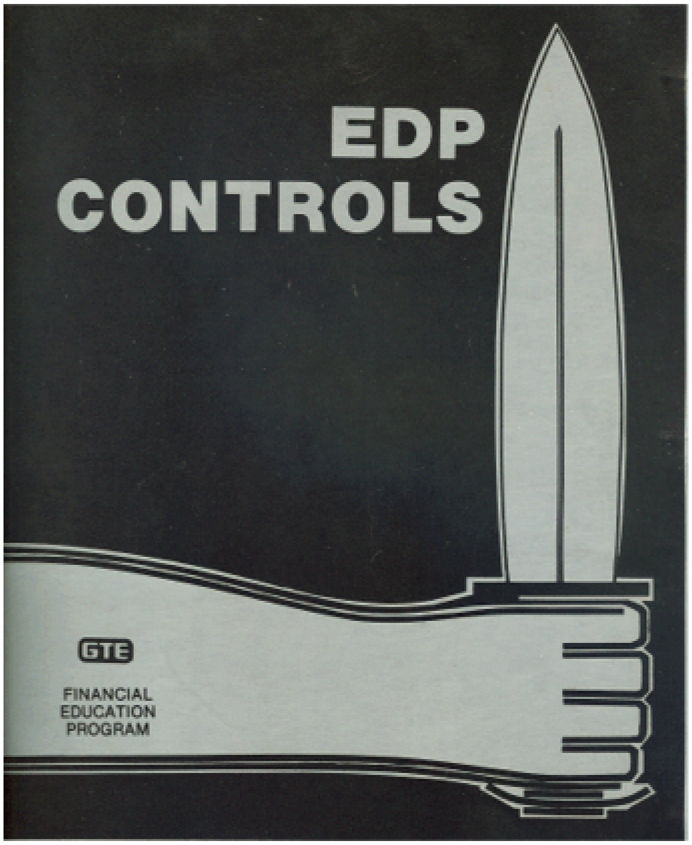
The Way-Back Machine

The year? 1979. The challenge? Educate and train managers in GTE's worldwide operations in EDP Audit and Control. Why? The Foreign Corrupt Practices Act of 1977, a United States federal law primarily known for two of its main provisions, one that deals with *accounting transparency* requirements of issuers required to report under the Securities Exchange Act of 1934 and another that deals with bribery of foreign officials.

When asked to lead the team to develop GTE's EDP Audit and Control course, I thought, "Uggh, how boring." By the way, for you younger readers, EDP means Electronic Data Processing, the forerunner to today's IT nomenclature. At the time, my peers and I were into exciting things like timesharing, the computer utility (the forerunner to today's On-Demand), packet-switching nets (we actually used Internet technologies back then, as Larry Roberts, one of the originators of the

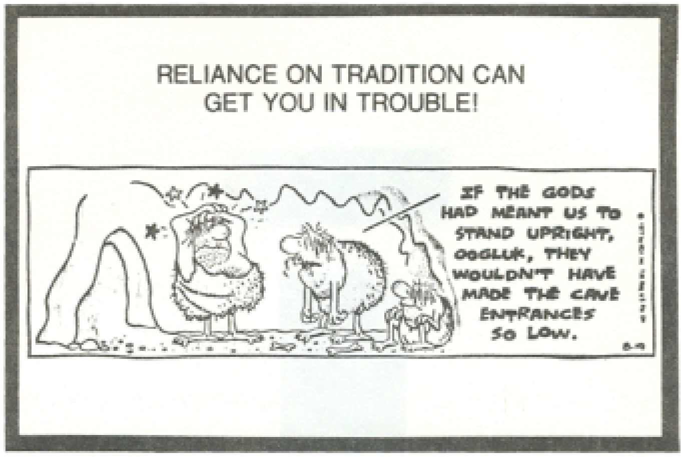
Internet was on board), and APL programming. So, back to the awful idea of that EDP controls thing. Boring? Not!

With source materials from the landmark, “Systems Auditing and Control Report” (the SAC Report) from SRI International, and the 1978 book, *Crime by Computer*, by Donn Parker, we had a complete Sherlock Holmes experience. We even recruited William Perry, Director of Research at the Institute of Internal Auditors, to produce a 15 minute video, “Bonnie and Clyde University,” where students were taught how to use the “salami technique” (how programmers at banks could use the rounding in interest calculations to shave off fractions of a penny and post it to their own bank accounts, adding up to big bucks in their accounts) or how to use the “pizza ploy” to gain entry into secure data centers (dress up as a pizza delivery person, ring the bell with a hot pizza in the other hand, and you are in). What interesting stuff in what I had thought would be boring back office auditing stuff.



1979 EDP Controls Course

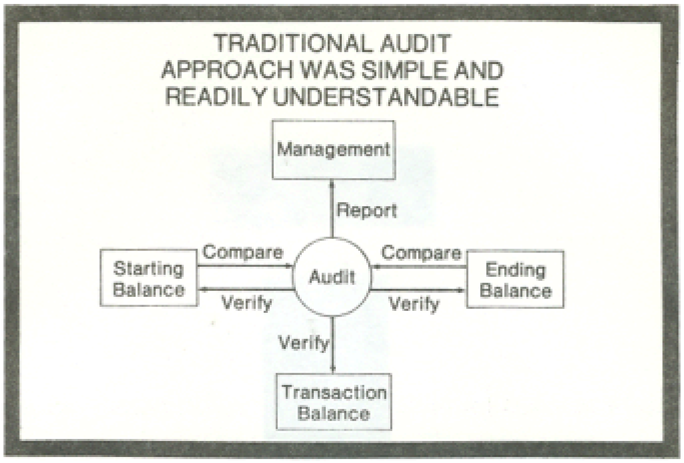
There was, of course, serious content in our EDP Controls course. Because technology had changed from batch mainframe systems to online transaction processing with those ubiquitous green-screen terminals, new control techniques were needed to address those nine loss exposures that don’t go away with any new technology. The loss exposures remain; the control techniques are what must change. Further, relying on the traditions of the past technology can indeed get you in trouble. For example, even though companies had tight access controls over their data centers in the era of batch processing, you didn’t even have to pose as a pizza delivery person to gain entrance with the advent of online terminals and online transaction processing.



RELIANCE ON TRADITION CAN GET YOU IN TROUBLE!

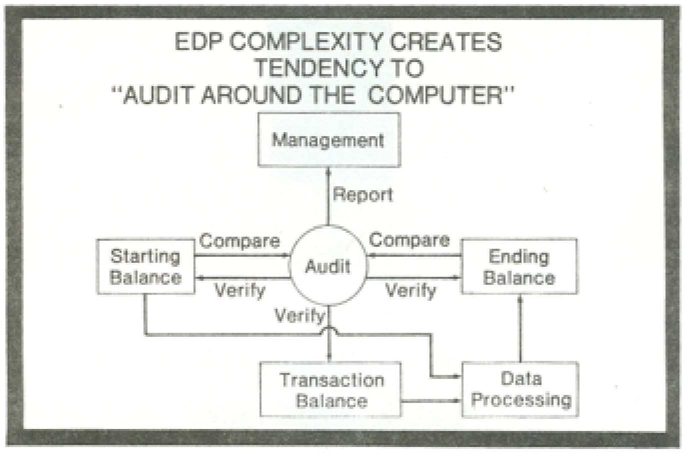
IF THE GODS HAD MEANT US TO STAND UPRIGHT, OOGLUK, THEY WOULDN'T HAVE MADE THE CAVE ENTRANCES SO LOW.

What were the lessons learned from the 500-company SAC study by SRI International? The key lesson was that auditability and control of business systems could no longer rely on traditional means, matching starting balances with transaction journals to validate ending balances.

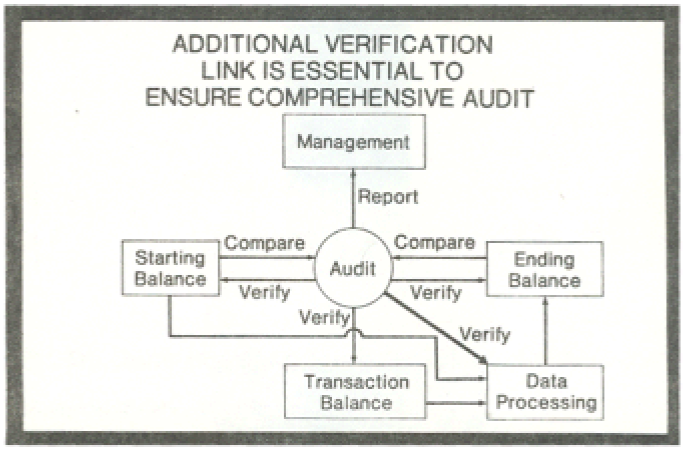


TRADITIONAL AUDIT APPROACH WAS SIMPLE AND READILY UNDERSTANDABLE

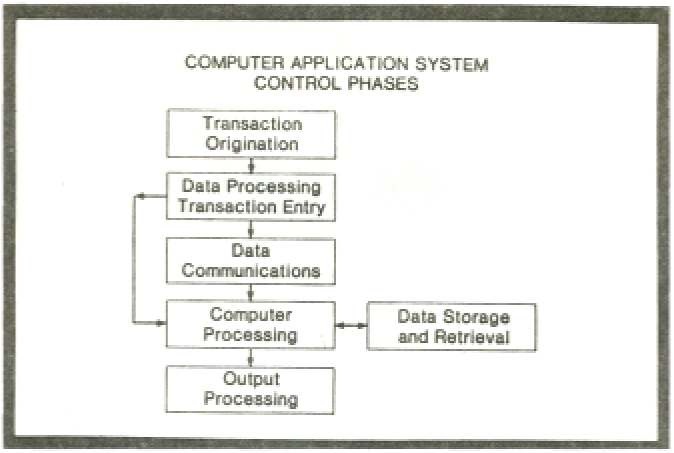
But tradition was hard to break, and companies essentially clung to tradition and “Audited Around the Computer.” That is, auditors simply looked at the transaction journals now maintained by computer systems instead of paper trails, but they did not go inside the computer “processing” to see what was happening. That’s how, for example, smart bank programmers were able to shave off mills for interest calculations and deposit an aggregate of large sums in their personal accounts, as starting and ending balances remained in synch. No one had a clue that mills were being milled away into personal accounts.

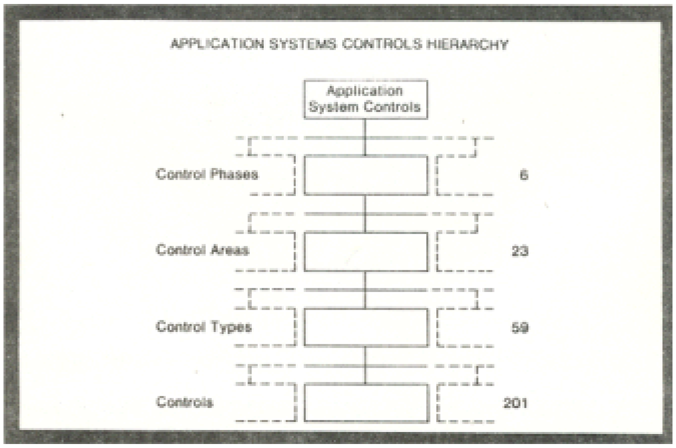


The lesson learned and brought to light? A company had to place auditability and controls "inside the computer," or, more specifically, inside the computer applications themselves using "transaction flow analysis."



In the techniques of transaction flow analysis, six phases were identified that further involved 23 control areas, which, in turn, could involve 23 control types and 201 possible controls. Risk analysis governed the appropriateness of controls selection.


COMPUTER APPLICATION SYSTEM CONTROL PHASES
Transaction Origination
Data Processing Transaction Entry
Data Communications
Computer Processing
Data Storage and Retrieval
Output Processing


APPLICATION SYSTEMS CONTROLS HIERARCHY
Application System Controls
Control Phases
6
Control Areas
23
Control Types
59
Controls
201

Way back in 1979, this was some pretty complex stuff, but if companies didn't comply with the Foreign Corrupt Practices Act, not only the enterprise, but also individuals, could be prosecuted under federal law. But that complexity pales in light of today's process world where the "process" supersedes the "application" as the object of auditability and control, and an end-to-end business process may encompass many companies and many countries and many laws. Oh my.

Fast Forward to 2007.

The Sarbanes-Oxley Act of 2002 (also known as the Public Company Accounting Reform and Investor Protection Act of 2002 and commonly called SOX or Sarbox) is a United States federal law enacted on July 30, 2002, in response to a number of major corporate and accounting scandals including those affecting Enron, Tyco International, Peregrine Systems, and WorldCom. These scandals resulted in a decline of public trust in accounting and reporting practices. Sarbox has not only been one of the major selling points for BPM vendors, it has also been one of the reasons some companies have registered with foreign security exchanges instead of the U.S. exchanges.

But, aside from these facts, what's really at issue is, as I'll repeat from the email I mentioned earlier, "How to create ad-hoc work environments across company boundaries and still maintain the security posture of each company seems to be a glaring issue …."
Stated in other words, how do companies provide auditability and controls when end-to-end business processes that span multiple organizations are the object, not individual applications inside a single company? Where are the "Process Auditability and Control Reports" for 2007? How does a company audit "through the end-to-end process" instead of around it? Where are the kinds of internal controls placed in "applications" to be placed in "end-to-end business processes?"

Far too often, in the nascent world of multi-company process management, security alone gains the most attention. The standard AAA metaphor (Authentication, Authorization, and Accounting). But AAA just skims the surface. Current attempts to provide an Internet-scale security framework, such as that by the Liberty Alliance, are low-level and technical. They focus on Authentication. Meanwhile, the aspects of such frameworks that claim to handle Authorization and Accounting are facile and certainly not industrial strength.

As a result, Authorization and Accounting have basically not moved on since the 1980s. Ross Anderson's seminal work, "Security Engineering," was published in 2001, but most of it could have been written ten years before. Experience teaches that ERP systems access control, as currently implemented, is not only extremely hard to configure but almost unworkable in practice. As scores of organizations worldwide can tell you, almost everywhere, people work around access control, sharing passwords like mints! If they didn't, they wouldn't be able to get their work done.

The root of the problem is that Authorization and Accounting of collaborative work must be *process-based* to be effective. Further, the process "model" must properly explain and support what is going on. Otherwise, how is a system administrator to know in advance whether it is valid to allow transfer of document A to IP address B from account C in domain D? And what does the audit trail of such a transfer tell anyone? Without an appropriate process context, nothing makes sense, and this context depends not just on the process type (Widget Sale) but also on the process instance (Sale to ABC of Widget PQR by sales team XYZ starting DD-MM-YYYY).

There are many challenging problems for the auditability and control of end-to-end business processes that involve human collaboration. Perhaps the most challenging is delegation of authority. As explained in the book that defined "human-driven processes," *Human Interactions* (Keith Harrison-Broninski, 2005, Meghan-Kiffer Press): "In real life, it is common for one process participant to offload a particular piece of work to another, perhaps adding a new person to the process specifically for this purpose. In a process support system, this can be done by starting a child Role, and passing across to it a specification for some work, along with the resources necessary to complete it: An architect working on a skyscraper may commission lobby furniture from another architect, for example, or a graphic designer request a particular graphic from another designer.

"Suppose that one resource passed across to the child Role is a communication channel with a supplier, for example, of construction materials or stock photos. How does the supplier know that a request received from the delegate is to be trusted in the same way as a request from the original architect or designer? Can the supplier even tell the difference? Once the job is finished, should they still respond to communications from the delegate? How do they even know when the job is finished?

"These questions are complex, and the subject of current academic work at a high level. We made reference earlier to the graphical theory of *bigraphs* by Robin Milner (inventor of the pi-calculus) and Ole Høgh Jensen, who are attempting to provide a formal underpinning for computation that deals with the relationship between 'locality' and 'connectivity'—between *where you are* and *what you can access.*[i] In the long-term, such work may provide generic answers. In the short-term, the solution lies in providing *process support* that caters specifically for delegation, and provides tracking mechanisms to deal with it.

"One thing is certain. Sooner or later, you'll have to use *process support* to deal with distributed access to systems. In the world of the networked supply chain, no company is an island. Eventually, unpalatable as it may seem, particularly to IT staff, you have to open up your systems to the outside world, not just for viewing data, but for others to create, edit, and delete it.

"Massive security problems are inevitable. In the best case, the problems will simply be overworked systems administrators. The worst case could put you out of business. A way forward is needed which reduces the maintenance overhead while guaranteeing full control over access. The most promising is to combine *Role-based process support* with an authentication system.

"The companies that develop and implement such technology will find themselves way out ahead of their competitors. They will be able to open up their systems to partners without strain and with a level of worry that is minimized as far as possible. In particular, the problem of *confidentiality*, currently unrecognized due to lack of any practical solution, will be resolved rather than exacerbated. If you want to become a real-time enterprise, this is where to start."

Human Interactions: Now things get real interesting.

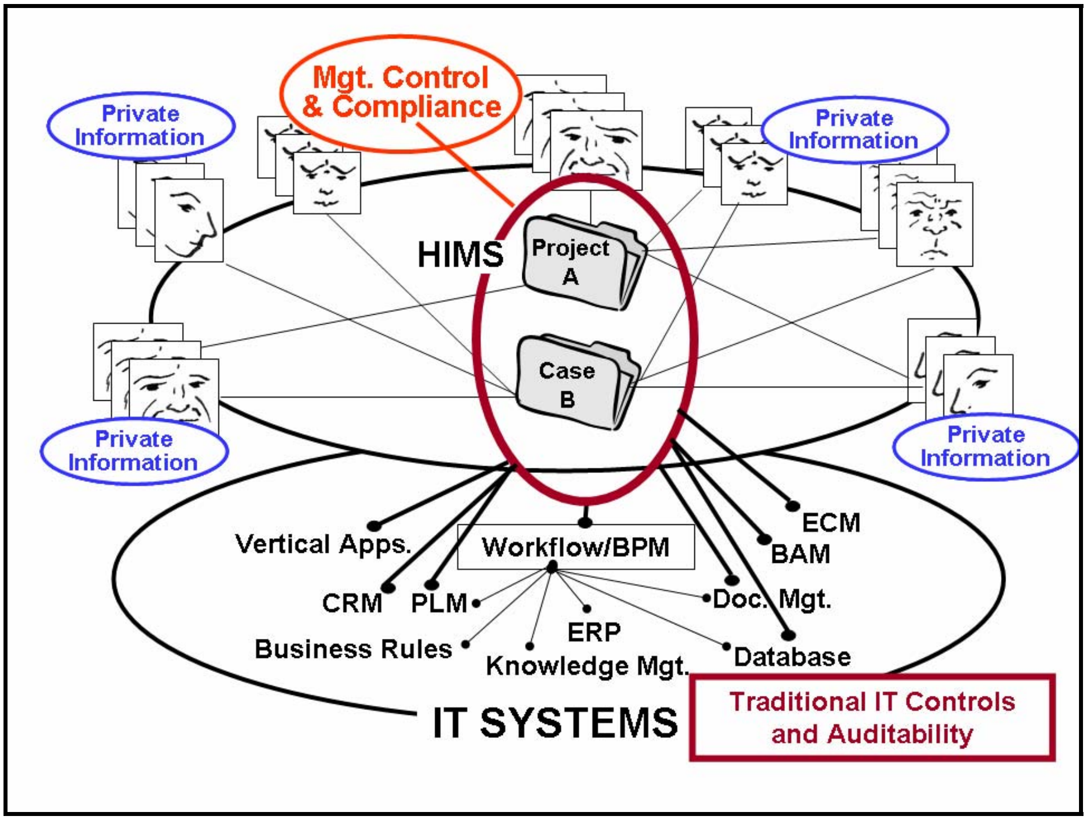
As I mentioned, Sarbox compliance has been a major selling point for BPM vendors. Why? For starters, workflow-style BPM systems leave clear audit trails, as workflow structures are predefined and thus straightforward to control. Workflow, as with many other types of computer applications implement many of the traditional IT control and auditability features that have evolved over the years. But what about that vital link in business processes, the human interactions where the structure emerges as the process is born and changes in-flight with participants dropping in and out of the shared process workspace somewhere in cyberspace?

Let's return to the book, *Human Interactions,* for more insights, this time on the need for role-based process support and confidentiality. "A simple way to think about Roles is in terms of files – not documents on a computer, but old-fashioned box files. People naturally keep related items and papers together, if they can manage it. If the objects in question are on a computer, they group them into directories, folders, or branches on a tree. If the objects are physical rather than virtual (atoms rather than bits), they put them in the same box. If and when such systems break down, it becomes hard to carry out the work to which the objects are related – and if this has happened at all, it often means that the work has *already* gone astray, and that things generally are in a muddle. This tells us that proper division of information is linked intimately to proper division of behavior.

"Based on this principle, a reasonable way to start dividing up behavior into Roles is by dividing up the information used in each one. This applies whether you are an analyst trying to understand a specific business process, or an individual trying to understand his/her separate responsibilities within an organization. A reasonable mental image of a Role is a *desktop* or an *office*, containing a specific set of documents and other items (keys to machinery, rubber stamps, communication devices, symbolic badges of status, etc.).

"Taking this paradigm further, we can say something very interesting about Roles. *Their information is private."*

I've illustrated this private nature of information below by annotating a figure from my BP Trends column, "The Greatest Innovation Since BPM," (http://tinyurl.com/37vklq**)** where I discuss the human interaction management system (HIMS) and its relationship to traditional IT systems, including workflow-style BPM.



Harrison-Broninski again: “You do not expect other people to come up and remove – or even read – documents on your desktop without explicit permission. In other words, others do not have access to information resources within one of your Roles. If and when you wish to share information, you do so by sending it to someone, or by showing it to him or her. Moreover, once you have shared information in this way, allowing people to take it away for their own use, you do not expect their copy of the information to remain the same as your own. You might email them a draft of a memo, then carry on working on the original, for instance, or send a status report on a certain date that carries on being updated daily at your end. This assumption is absolutely basic to human behavior. We all like – and need – to remain in control of the information we use.

“There are many reasons for this. For one, to share information with someone is to release it from your control to some extent, and we need to prepare for this – make sure that we are happy with what goes out – before letting it go. For another, much information is sensitive, and we need to make sure that only the right people see it, at the right time, with the right guarantees of security. There are also implied commitments made by sharing knowledge. For example, telling a supplier that you are looking for a partner on an important project might well give them the idea that they are being considered as the potential partner, with the result that they invest time and money in preparing for the project. It would be irresponsible, and detrimental to future relations with the supplier to give them such information if you had no intention of giving them any chance to bid when the time came.

“Understanding that the information each Role uses is *personal* to that Role has yet deeper significance. Information takes different forms on different desktops. Almost the first thing that anyone does on receiving a spreadsheet, for example, is to reformat it to show the rows and columns they are particularly interested in, perhaps with highlighting or filtering in places. They may also add additional data that was not included in the original spreadsheet – information they are privy to that possibly was not available to the originator of the spreadsheet, or information they generate while working – the status of each item, for example, or just free text notes.

“The spreadsheet example is just that – an example. The principle that data formats vary between Roles applies to almost any form of data held within a Role. Even structured data that comes from a computer system is no exception.”

Getting Started.

Make no mistake: The safeguarding of confidential commercial information is a headache of such proportions that, the more you think about it, the less you want to think about it. The problem is not related specifically to IT, of course. Security, by nature, is a multi-faceted issue, with aspects that range from highly technical questions of cryptography through to ensuring that, when entering a building, people do not hold the door open for the stranger walking behind them. Now multiply these concerns by the millions of doors scattered across the Web.

The use of Roles as the foundation for process definition offers a way forward for determining *who should be able to access what*. A great starting point to drill down on the use of roles in control of system-to-system (S2S), human-to-system (H2S), and human-to-human (H2H) inter-enterprise business processes, both ad-hoc and predefined, is the understanding you can gain from two major books. The first is the one I quoted from above: *Human Interactions: The Heart And Soul Of Business Process Management*, by Keith Harrison-Boninski (www.mkpress.com/hi). The second is the book whose author draws inspiration from 20 years of research into how to tackle dynamic work collaboration with computer-based support: *Business Process Management: A Rigorous Approach*, by Martin Ould (www.mkpress.com/ OULDdesc.html).

Harrison-Broninski focuses squarely on human-driven process issues, setting out a framework that solves many of the security problems described above, while Ould provides an all-embracing treatment of organizational processes – in particular, a generic way to derive your “process architecture.” Both men were working on IPSEs (Integrated Project Support Environments), actually prototypes of BPMS software, in the mid-1980s, and their current ideas are opening up the way for a new generation of process support methods and techniques. You can find a short description of how Harrison-Broninski’s *Human Interaction Management* theory intersects with Ould’s *Riva* method at http://tinyurl.com/2dqatp.

Returning to my opening comments about growing concern over the challenges of security, control, and auditability of multi-company, end-to-end business processes that strike fear in the hearts of business executives, it’s time for the BPM industry and BPM professionals to go beyond traditional IT control and audibility (from certified EDP Auditors to certified BPM Auditors). It’s time to address controls associated with conversations for action and other forms of negotiating and committing to agreements made among parties scattered across the globe. It’s time to provide audit trails of who-what-when-where-and-why interactions that take place in cyberspace. It’s time to give workers explicit control over access to their private information in a way that parallels the control they have over their physical desks and their PC desktops. It’s time for a new edition of the 1977 Systems Auditability and Control Reports that addresses the nine fundamental loss exposures in relation to shared workspaces where no one company owns the end-to-end business process. It’s time to give business executives the confidence they need to further invest in ever more complex business processes that span the globe. What I thought, mistakenly, would be a boring subject in 1979, EDP Controls, promises to be ever more fascinating – and ever more urgent – today.

[1] Jensen, O., Milner, R., 2003, "Bigraphs and mobile processes," University of Cambridge Computer Laboratory