Central Banking and the Information Technology Revolution: Challenges and Opportunities

Remarks of
Bruce J. Summers
Director
Federal Reserve Information Technology

Bank of Japan
Conference on the Development of
Information Technology and Central Banking
Tokyo, Japan
October 2, 2000

Central Banking and the Information Technology Revolution: Challenges and Opportunities

Thank you Mr. Matsushima and good morning, ladies and gentlemen. It is a pleasure for me to join you at the Bank of Japan conference on information technology development and central banking.

I would also like to thank Mr. Iwao Kuroda, Executive Director of the Bank of Japan, who first approached me about participating in this conference. Mr. Kuroda and I have worked together over the years on a number of initiatives, both multilaterally under the aegis of international financial institutions including the Bank for International Settlements and the International Monetary Fund, and bilaterally on matters of mutual concern to our respective central banks. Through this work I have gained great respect for the Bank of Japan's progressive interest in the use of information technology to advance the development of central banking in a range of subject areas, including the payment system. It is therefore a special honor for me to participate in the Bank of Japan's conference on the development of information technology and central banking.

This conference is organized specifically for the benefit of central bankers from the Asian-Pacific region. Yet, in matters involving information technology, central banks worldwide, and the financial economies they support and in which they participate, have much in common. Accordingly, my remarks today are intended for the broad central bank community. In particular, I hope to promote understanding of the challenges and the opportunities faced by central bankers in managing the changes in our businesses which are being brought about by the information technology revolution.

My purpose this morning is twofold. First, I will identify the broad challenges central banks face in responding to the information technology revolution. There is, of course, no shortage of attention to the dramatic effects that technology innovation is having on our economies and even on our more basic social structures. One challenge central bankers face is adapting their own business processes in ways that are progressive and responsive, so that they remain relevant in the information age. Another challenge, however, and one which I believe receives insufficient attention, concerns the lack of readiness of some new technologies for production use in mission-critical infrastructures, including the financial infrastructures which are the responsibility of wholesale financial institutions. Second, I would like to offer some views, based on my experience with information technology, as to how central bankers can exploit the opportunities offered by the technology revolution in our business processes and operations, while at the same time exercising sound judgment concerning the introduction of new technologies.

I will organize my remarks according to four topics. First, to help establish my point of reference, I will provide a brief overview of how Federal Reserve System information technology is now organized by the 12 Federal Reserve Banks. Second, I will address the importance of integrity and trust in central banking--including the integrity of operations and the information technology infrastructure. Third, I will identify the principal information technology directions that define the "revolution" which we face. Fourth, I will explore the implications of these new technologies for central bank businesses, and the challenges and opportunities that these new technologies pose. In the process, I will share my conclusions about what constitutes the "ground truth"--to borrow a term from the knowledge management field--that we all need to manage by as we adapt our business practices to the information technology revolution.

Federal Reserve Information Technology Organization

My frame of reference for thinking about technology issues is principally that of the Federal Reserve banking system. As you know, the Federal Reserve is a very hands-on, operational central bank with a significant role in the U.S. payment system, in financial markets more generally, and in bank supervision. I would like to provide some insight into how the 12 Federal Reserve Banks have organized themselves for purposes of managing information technology to support their responsibilities. As I do so, please keep in mind that the 12 Federal Reserve Banks compete with private banks and data processing services companies in the provision of certain financial services and are increasingly subject to market forces, including intense competition attributable in part to the increased market efficiency afforded by technology innovations. These market forces include keen price competition and time-to-market considerations.

The 12 Reserve Banks have centralized a considerable portion of their national or Systemwide information technology activities into an organization called Federal Reserve Information Technology. This national organization is comprised of two principal business units: Information Technology Planning and Standards, and Federal Reserve Automation Services. The former is responsible for the enterprise-level IT architecture and internal IT standards which apply to business units and their business software application developers Systemwide. It is managed by a senior official equivalent to the chief technology officer in a commercial institution. The latter is our internal services company, responsible for providing utility-like communications and processing services to the 12 Federal Reserve Banks. It is our digital power plant, if you will. It is managed by a senior official equivalent to a chief operating officer in a commercial institution.

Oversight and governance of information technology in the Reserve Banks is an executive function. In fact, the Federal Reserve Bank presidents, who are the CEOs of their respective banks, have established a governance arm analogous to a board of directors, called the Information Technology Oversight Committee (ITOC), to which Federal Reserve Information Technology is accountable (there is an additional, legal governance connection to the board of directors of a single Reserve Bank, but this relationship is not significant for our purposes here).

In September 1999, the Reserve Bank presidents adopted business first principles, which set a general, Systemwide direction regarding the management and use of information technology by Federal Reserve business functions. The seven business first principles are attached to my remarks. One of the most significant principles, in my view, is the fourth, which states that the Reserve Banks will lead business innovation in ways that contribute to and enhance national operations. Underlying this business principle is a very important aspect of the Federal Reserve's organizational design, namely, the location of business application software development within the Reserve Banks, where it is closest to business lines and customers.

We place an extremely heavy emphasis on strong and effective governance over our Systemwide, centralized information technology operations, analogous to corporate information technology in the private sector. All information technology operations, and all investment in information technology wherever located, must be consistent with our enterprise-wide information technology architecture, which is a responsibility of our chief technology officer. Because our investment in shared infrastructure is so large, ITOC plays a very active role in approving the high-priority objectives of Federal Reserve Information Technology and, then, in assuring accountability for the achievement of these objectives by management. In my organization, we reflect the high-priority objectives wherever possible in personal performance evaluations of our officers and employees, and often encourage achievement of these high-priority objectives through specific performance incentives as a supplement to base compensation.

We also have very strong operational and financial control systems in place, together with robust and independent internal audit, as well as external audit capabilities. A Federal Reserve Bank general auditor has been assigned responsibility for audit of the Federal Reserve Information Technology organization. The professional audit staff dedicated to this function are as skilled and well trained as are our technical professionals, and the audit activity is well funded with a budget of approximately $2 million.

Finally, I think you will be interested in knowing that we regularly benchmark our operations to the private sector. This summer, for example, we completed a performance improvement study of data center operations by a well-known international firm which compared us to a "best" and a "most secure" reference group of private firms. These periodic benchmarking exercises have a direct influence on how we conduct operations. For example, a benchmark study of our national network several years ago led us to redesign our network support processes based on frame relay and Asynchronous Transfer Mode (ATM) technology. Further, this performance improvement study led us to outsource some network engineering and certain network operations functions. We determined that our basic business requirements for low cost and quick time-to-market for new services could best be met by a firm specializing in telecommunications.

Integrity and Trust in Central Banking

At a recent business and technology conference for Federal Reserve System staff, Vice Chairman Roger Ferguson of the Federal Reserve Board gave a keynote address in which he stated that one of the greatest assets of a central bank is its reputation. Such a characterization is completely appropriate and, in my view, applies not only to core central bank functions but to a support function such as information technology as well. There is a direct connection between a central bank's reputation and the integrity of its operations, including its information technology operations.

I think of the financial system as being comprised of six major components. These include deposit-taking and account-holding institutions (private banks); a central monetary authority; exchanges and clearing organizations that support trading, clearing, and settlement of transactions; laws and regulations that govern financial relationships (the rules of the game); a supervisory apparatus for maintaining order; and a technical apparatus that all of the other major components utilize. All central banks make a contribution in one or more of these areas, and most of our central banks have responsibility for part of the technical apparatus. Central banks, of course, are the final settlement authorities for the complex and sizable flows of financial transactions through their national economies. Obviously, operational integrity--including the highly reliable operation of the information technology infrastructure supporting the settlement of financial markets transactions--is essential to the reliable, orderly operation of a nation's banking and financial systems. Accordingly, operational excellence has a strong bearing on the public's overall perception of the central bank reputation. Because reputation is a key central bank asset, operational excellence and the responsible management of information technology in particular must be accorded special place. While I will not develop the theme here, I have in the past focused specific attention on the role of operational integrity in ensuring the public's trust, especially during a time of rapid change in technology, insofar as this involves electronic banking.[1]

Information Technology Directions

The basic challenge we, as central bankers, face is to manage responsibly the sweeping redesign and conversion of our business processes and supporting technological apparatus in response to the technology revolution. Financial services firms worldwide are restructuring (some would say reinventing) themselves around new business models driven by a number of factors, including the opportunities offered by new technologies. In fact, many financial services firms are becoming e-business companies by driving down their costs and increasing customer service through the application of technology and business process reengineering. For example, new technologies allow costs to be reduced through compression of the supply chain, to eliminate all redundant and non-value added steps between demand and its fulfillment. Further, customer service is enhanced by making valuable business information available quickly, easily, and in a meaningful presentation format both to the employees serving the customers, and to the customers themselves.

I would characterize the technology revolution which is leading the restructuring of the financial services industry as a paradigm shift involving both computing and communications. We are quickly transitioning from computer-

[1] Speech by Bruce J. Summers, "Integrity and Trust in Electronic Banking," 1999 Software Engineering Symposium, Carnegie Mellon Software Engineering Institute, September 1, 1999.

centric to network-centric designs and from closed to open systems. Underlying the paradigm shift is a fundamental change in the basic computing architecture, which is itself explained by rapid-paced scientific discovery and product development. Systems and software designers throughout the financial sector are embracing the main features of the new architecture. Two of these main features are distributed computing, which allows separation of distinct processing steps (for example, execution of business logic, administration of data, and presentation of information to the customer) into different "tiers" of an n-tier architecture, and information security models based on public key infrastructure, or PKI.

Concurrently, software design has been reformulated along the lines of the component model, and our traditional notion of the "software house" is shifting to that of the "business-component factory." Today, software is being developed based on logical components, and managers responsible for this development are placing emphasis on producing code that is transportable across the layers of the n-tier architecture, and that is reusable among business applications. Application software development which is based on the business-component factory model strongly supports business objectives of cost efficiency, enhanced customer service, and quick time-to-market.

The information technology revolution is, of course, also characterized by dramatic improvements in computer processing, telecommunications, and data storage. In each case, there are exponential improvements in performance accompanied by plummeting unit cost. As well, the advances in these three areas make it possible to access, transfer, and process information across heterogeneous systems.

Shifts in technology such as those described above have, of course, resulted in dramatic changes in business processes and therefore in business partner relationships, including relationships between central banks and the institutions they regulate, central bank services users (including the Treasury), and the general public. Within the Federal Reserve, for example, there has been a sharp increase in information sharing with the general public, regulated entities, a variety of commercial institutions to which we provide services, and sister central banks worldwide. Thus, the lines between internal and external customers are blurring. Network-centric computing and open-system architectures have greatly facilitated such information sharing. At the same time, increased opportunities for information sharing enabled by new technology pose a significant challenge in terms of protecting the security of business information, a theme that I will develop later. Suffice it to say for now that the concept of business-to-business electronic commerce has as much relevance for a central bank as it does for a private business.

To illustrate the importance of these technology directions for the Federal Reserve, I will refer to the architectural makeover from our legacy production and delivery platform to our new technology target platform. The main components of the legacy platform involve the mainframe computers and applications, a proprietary communications network, and proprietary thick client software used by our commercial bank business partners. As shown on the attached diagram, the target platform still includes the mainframe legacy applications (with over 90 million lines of code, it is highly likely that the mainframe applications will be around for some time to come). Significant new segments of the target platform include middleware added to translate between the mainframe protocols and those relied on in the n-tier architecture; a new web applications infrastructure, including new authentication (PKI) and authorization (role-based access control) security segments; and a very thin (let me say anorexic) browser-based client which is based on commercial off-the-shelf (COTS) browsers. At this point in time, I believe that the target platform will be able to meet the business requirements of all but the highest risk and most mission-critical applications.

Implications of New Technologies for Central Banks

The target platform shown in the diagram is an operational reality. The middleware component is in place; two certification authorities have been put into production, together with related security elements including a role-based access control system; and several applications ranging from check imaging to statistical reporting are being piloted. Nonetheless, we still think of this new platform, which is based on Internet and web technologies, as a target platform because some of its major components are not yet ready for "industrial strength" applications. For now, we are limiting use of the platform to low- and medium-risk applications. At this point, the combination of new technologies making up the target platform is a long way from being a perfect substitute for our legacy system in terms of reliability and security.

There is not time here to identify fully, much less address, the many types of challenges which the new platform design poses, for they are myriad and diverse. They range from the minutely technical to the broadly philosophical and may even combine these qualities. For example, we have identified a number of deficiencies, and even defects (principally involving security), in browsers since they are created primarily for recreational and mass-markets use, and not for wholesale financial markets. Moreover, their goal is to be maximally user-friendly in their target markets. While I believe we need to leverage the power and flexibility made available by these user-friendly and ubiquitous products, I also believe we should be exceedingly careful in relying on them for mission-critical applications. One action we have taken to help manage the technology risks posed by using open-market products is to engage in discussions with the vendors, both to lodge our concerns and influence development of product features and to assess independently the technological integrity of their products.

Broadly speaking, the new technologies act as enablers of our central banking business vision. They do this through instantaneous and extensive networking, tailored security for information assets, and greatly enhanced business functionality. Business information is a core asset for central banks, just as it is for all information-intensive firms. With the information at the core of our business model, we can define our networks to support sharing of information among applications, and we can customize security to protect our information assets. In other words, we implement value-added applications in which our unique information assets have been put to use. To help you understand what I mean by this, I think it would be useful to describe briefly how business information is shared, protected, and applied in value-added business processes during the "information age." In doing this, I will also identify some of the key technology enablers that allow us to achieve this new business vision.

Starting with the maintenance of information itself, many of us have devised information architectures which are essentially collections of silos of information. This de facto mode is in part a result of both traditional organizational structures and technology limitations. The problem we face is sometimes referred to as the "data in jail" problem. In contrast, the new vision is that of a single-source view of information. Some of the technology enablers that allow us to realize this vision are software business components, middleware, directory services, and advances in storage including storage area networks, network attached storage, and the like.

With respect to business networking and sharing of information through communications systems, our tradition and experience principally have been with proprietary protocols and point-to-point communications systems. Of course, the Internet has "changed everything," and the networking vision, as it is generally articulated today, involves open communications. The technology enablers which allow realization of the vision include virtual private networks, the use of public network services, and, of course, the TCP/IP and web protocols.

With respect to the protection of our information assets, many of us have traditionally operated under what I will call the binary trust model. Under this model, one is either trusted or not trusted; that is, one either has or does not have access to designated sets of business information. The new vision is for trust relationships based on graduated degrees of trust. We want to provide our business partners with access to selected information on a very graduated or granular basis. The technology enablers that allow us to achieve this vision include public key infrastructure (PKI), directory services, and new authentication and authorization methods such as digital signatures.

Finally, there is the ongoing, value-added use to which we put our information assets. Many of us have a tradition of building our own business applications, and we have done so under a systems paradigm based on a highly integrated vertical stack of applications and environmental support. This is the mainframe paradigm. In it, all of the parts of the delivery system are intricately related, from hardware through network through environmental and application software. The vision is reuse of software components and interoperability among the various layers of the technology stack. The vision is founded on the notion of open systems standards, and the technologies which let us achieve this vision are software component models, the n-tier architecture, and, of course, inexpensive and secure networking. Realization of this vision will reduce our dependency on a single or small set of vendors, thereby increasing our access to innovations and new products across the technology marketplace.

Another basic change in technology direction involves increased opportunity to buy instead of build business functionality. In the Federal Reserve, we have almost always relied on our own resources for business application development. While I expect this model to continue to predominate over the next several years, clearly there is potential for more outsourcing of the key technology components. I should add a significant caution, however, which is that outsourcing introduces an entirely new type of vendor risk that needs to be managed. In no case should a central bank relinquish its responsibility to understand the basic technologies it may choose to outsource, and the central bank should, by all means, invest in world-class procurement, contracting, and vendor management skills as it increases its reliance on outsourcing. We can never afford to place blind faith in others' "black box" solutions to our mission-critical business challenges. Moreover, we must be able to assure that our vendors practice sound controls in design and manufacturing, and that their employees are held to a high standard of integrity.

At the beginning of my talk, I promised to share with you the "ground truth" that we all need to manage by as we adapt our business practices to the information technology revolution. It is derived from my practical experience in managing the introduction of new technologies into a central banking environment. The ground truth that I wish to share is straightforward: investment in new technologies is both risky and expensive. These "lessons learned" from experience are interrelated.

Both the technical and the popular press are replete with examples of Internet-based business operations which have faltered as a result of the breakdown of systems based on newer technologies. Some of the breakdowns are attributable to the stresses and strains of normal business operations, including processing peaks that crash systems; failures in change control processes during the upgrade to new versions of software; and, of more concern, inherent defects in the design of products widely deployed in the marketplace. As well, we have ample reason to be concerned about vulnerability to external (not to mention internal) attacks on our technology platforms, as evidenced by the recent spate of denial of service attacks over the Internet. Many, if not most, of the risks we face in managing newer technologies are very familiar from our experience with legacy systems; that is, many systems management practices such as change control do not lose their relevance as the technology evolves. Indeed, the tools to perform systems management for the newer distributed computing platforms are rapidly evolving but are still inadequate when compared to tools available for the legacy system.

There is, however, one extremely important new dimension to technology risk, and I have touched on it already: namely, the growing propensity of vendors to design and build products principally with the recreational and mass markets in mind. I am concerned that the needs of the commercial marketplace are not being addressed as they should be in product development, especially with regard to security features. I am also concerned by what may be a growing propensity on the part of businesses, including firms responsible for the financial infrastructure, to use information technology products that do not meet high enough standards of quality. We should be extremely concerned, and appropriately cautious, with regard to the degree of reliance we place on new products, especially products that may present a single point of failure in our production systems. I have already mentioned one example, namely, commercial off-the-shelf browsers. The need for prudence, however, applies across the full spectrum of products, including those deployed in back-end systems. To cite one more example, our experience with middleware has shown the robustness of the commercial versions of these products to be at least somewhat inconsistent with our high-performance standards. As a central bank operating mission-critical systems under heavy workloads, we find ourselves in the position of reporting a disproportionately high number of problems with middleware products. Such products may well suit the needs of many businesses, but we are finding that it is less and less realistic to expect that off-the-shelf products can be introduced into our environment and meet our high standards for security, control, and reliability without some degree of product modification and enhancement. As a consequence, we are placing renewed emphasis on the quality assurance processes as we apply newer technologies.

Investment in new information technology is not only complex but also expensive, and every responsible technology-based business strategy must be accompanied by a rigorous financial plan. As a general rule, sound management calls for retiring old infrastructure as part of the rollout of new infrastructure, thereby providing a source of self-funding for new investment. As public institutions, central banks are accountable for the stewardship of public resources and must practice responsible financial management. As suggested by the diagram, however, self-funding of new investments for an organization heavily invested in legacy infrastructure and applications is a difficult challenge.

For an established firm with a large investment in legacy systems, including millions of lines of mainframe-based application code, the immediate promise of new technology lies principally in enhancing the customer relationship. This implies the layering on, as opposed to the replacement of, technology infrastructure. The technology itself is expensive, and acquiring the competencies to manage the new technology responsibly is even more expensive. Accordingly, we must take a longer-term view of the business opportunities and develop multi-year financial strategies for rationalizing these investments. In this connection, we are all well aware that until recently the dot-com companies have seen little need to practice traditional financial disciplines. The reason is that the dot-com companies are by and large de novo firms, unencumbered by large investments in legacy technologies, and they have lots of capital to invest in their new infrastructures. Moreover, these firms and their investors have been betting on market expansion and the generation of significant new revenue streams as justifications for their wide-open technology investments. No longer is the "dot-com strategy" a sure bet. Such a strategy needs to be very carefully considered by any firm with a large investment in legacy infrastructure.

Concluding Comments

I hope that these remarks have provided a useful perspective on how central banks can best step up to the challenges and take advantage of the opportunities posed by the information technology revolution. Both the challenges and the opportunities are significant, although I would assert that at this point in time the challenges predominate in the case of organizations like central banks, which are responsible for the reliable operation of mission-critical financial infrastructure. Needless to say, as central bankers we share an important responsibility for maintaining the integrity of the financial infrastructure and for maintaining public trust in the integrity of the financial system. In the information age, the integrity of the information technology infrastructure assumes even greater importance.

The value-added contributions that we make in discharging our central bank responsibilities can be enhanced considerably through the realization of a technology-based business vision for the use, sharing, and security of business information. By carefully evaluating and experimenting with new technologies before introducing them into our mission-critical product infrastructures, we can exercise the prudence necessary to make successful use of innovations. As well, by carefully assessing the longer-term financial implications of technology programs, we will be able to manage appropriately the substantial investments that such programs imply. I have every confidence that we will rise to the challenge of being both progressive and prudent at the same time, thereby turning the promise of new technology to the public's advantage.

Attachments

Attachment

Business First Principles

1. We will provide operationally seamless supervision, services and support to multi-regional banking organizations.

2. Our security solutions will provide easy-to-use protections appropriate for each business function.

3. Our systems will integrate transactions and information to facilitate end-to-end business processes.

4. Reserve Banks will lead business innovation in ways that contribute to and enhance national operations.

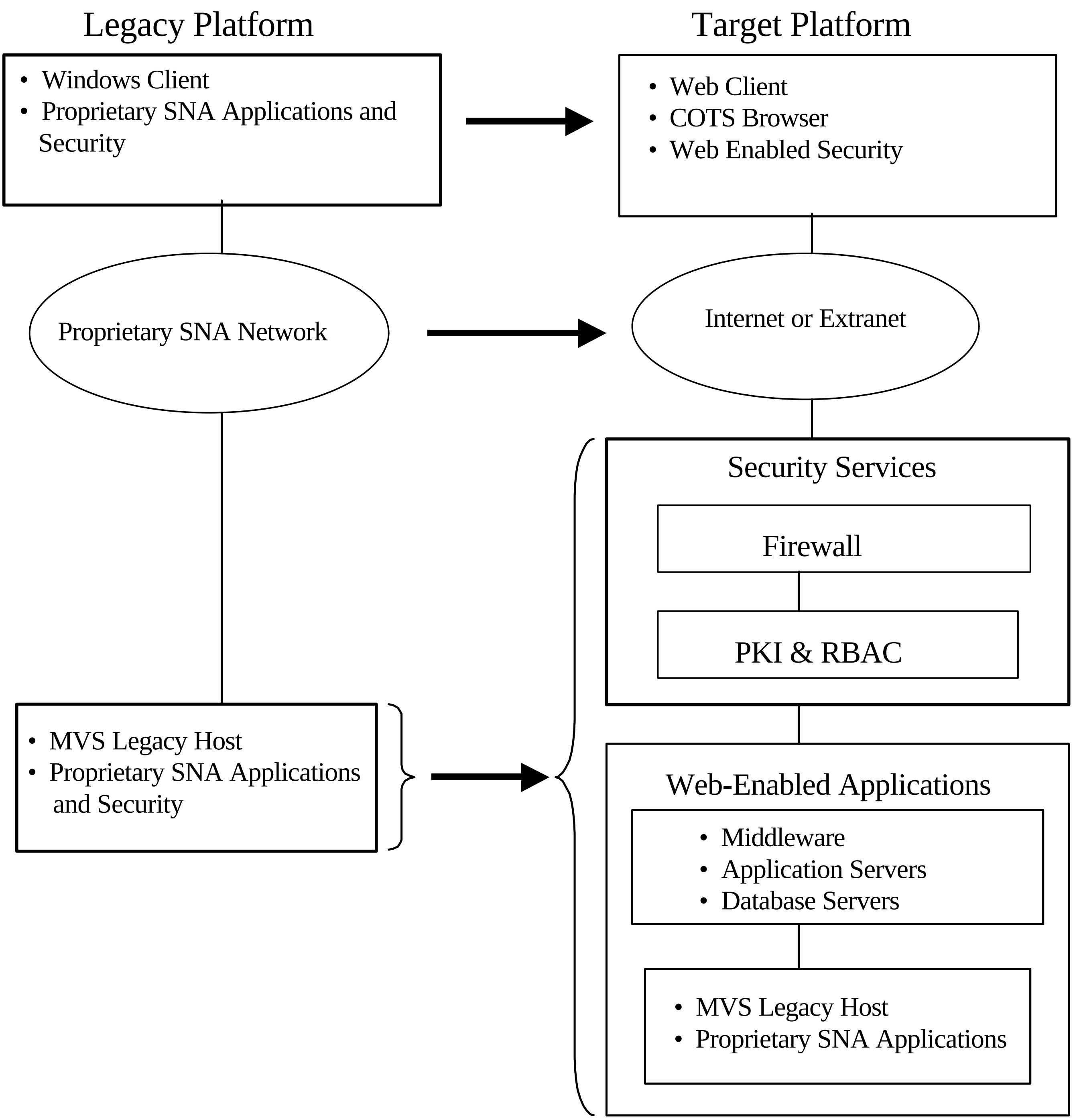
5. Our business rules, reporting and incentive systems will establish personal responsibility and accountability, and stress business value in the delivery of end product.

6. Technology experts will partner with business function leaders to anticipate business opportunities and challenges.

7. Our business plans and technology choices will support rapid time-to-market for policy changes and new products.

Attachment

Diagram
Comparison of Legacy and Target End-to-End IT Platform


Legacy Platform
Target Platform
• Windows Client
• Proprietary SNA Applications and Security
• Web Client
• COTS Browser
• Web Enabled Security
Proprietary SNA Network
Internet or Extranet
Security Services
Firewall
PKI & RBAC
• MVS Legacy Host
• Proprietary SNA Applications and Security
Web-Enabled Applications
• Middleware
• Application Servers
• Database Servers
• MVS Legacy Host
• Proprietary SNA Applications