CHAPTER

1

The Role of Information Technology Architecture in Information Systems Design

How many laws and regulations affect your business? How many of them affect your organization's computer applications? Do your computer systems comply with all of them? All are good questions with transitive answers. Sarbanes-Oxley (SOX) is one of many new regulations making its mark on how business is conducted. There will more new ones not too far down the road.

By taking action now in conforming to the mandate for adequate controls on information technology systems and applications required by SOX, you also position your organization to meet privacy protection mandates, disclosure requirements, and what may be needed for the next round of regulation that could affect your data systems.

Meeting the SOX Challenge

The Sarbanes-Oxley Section 404 requirements to maintain adequate security controls over information technology systems forge a challenging and perhaps somewhat intimidating task. Add to them a multitude of regulatory agencies at all levels of government that are endlessly generating requirements (federal HIPAA statutes and California's privacy protection initiative that requires

firms to make individual disclosures of known compromises to anyone's private information that might result in identity theft, for example) that your information technology security and privacy protection controls also must meet, and the whole undertaking could seem overwhelming.

With all of the sometimes confusing and often conflicting requirements placed on an organization's IT (information technology) practitioners today, charting a practical course for compliance with Sarbanes-Oxley seems very hard to achieve. IT managers face the ever-present need to provide easy-to-use applications on systems that directly support the business processes to efficiently get the work done. They also are now required to place on the end users and systems a set of controls that support and meet the requirements of the regulatory agencies. SOX brings all of the historical requirements of cash controls, accounting standards, and audit oversight and reporting to the micro bits and bytes information technology realm often ruled by a more laissez-faire approach to getting things done "yesterday if possible."

Understanding the New Definition of Adequate

The big story in Sarbanes-Oxley for the IT professional is that earlier approaches to quickly getting applications built and in place to support the business (punch a few holes in the firewall and worry about security later) will no longer pass the inevitable audit. Access controls that give everyone in the same OU (organizational unit container) the same access rights are no longer considered "adequate" security controls. Meeting the test of maintaining effective internal control structure and processes supporting accurate financial reporting requires treating SOX 404 compliance with a focus and discipline not always evident in existing information systems designs.

The annual audit findings that report substantial weaknesses in controls will attest to these shortcomings in existing IT designs in small and large companies alike. Looking forward, there's just no point to building tomorrow's audit failures today. Legacy systems and existing applications must be brought into compliance. Failure to do so has the potential of a big negative impact on the value of the public companies that do not meet the compliance tests during audits. Public audit of internal controls linked to Section 404(b) requires auditors to assess whether the internal control structure and procedures contain any substantial weaknesses of any kind. The audit reports are expected to attest to the success of the company's internal control structure and procedures for financial reporting purposes.

Any flaw in an organization's control relationship between identity, authentication, access control measures, and the links made to financial or privacy data are subject to audit and adverse reporting. As the rules are refined and auditors become more knowledgeable about the technologies involved, any imperfections in the controls will likely be discovered over time.

High Stakes for Compliance Failures

One could easily imagine a corporation that doesn't look too bad on its first audit, but some material findings emerge related to SOX 404 issues. The company fixes some things and then gets audited by a different team capable of a more detailed technology audit, leading to more negative findings in audit year two. The company fixes the year-two findings only to be audited in year three by yet another more sophisticated team, and behold, more negative audit findings related to the quality of controls. After a scenario like that, Wall Street analysts may feel compelled to point out to the stock-buying public that company X seems to be having difficulty correcting its compliance issues, and they may downgrade the outlook for the company because it just can't seem to get a grip on instituting the necessary controls.

The control issues surrounding compliance with SOX-like mandates do not apply only to public companies. Governments at all levels, the nonprofit sector, and closely held companies all face the need to satisfactorily protect the integrity of their confidential information and provide adequate controls on access to data stores and to counter the liability of losses of clients and members personally identifying information. For some nonprofit organizations, the financial risk of litigation resulting from inadequate controls may be far greater than any harm from adverse audit findings.

This book is intended to help those responsible for establishing and maintaining adequate information technology security controls. The information applies regardless of the kind of business. As the oversight and regulation environment is perfected, it will inevitably require organizations of all types to put in place controls that will be deemed adequate for compliance with SOX, HIPAA, or other oversight entity's rules. Even if the controls are not required by laws or regulations, it simply makes sense to implement and maintain sufficient controls for just generally protecting privacy information or access to confidential or valuable information.

Examining the Role of Architecture

Using ITA (information technology architecture) design concepts and the documentation used to express IT design is the only approach to successfully bring existing or new applications, systems, or networks into the condition of having an "adequate internal control structure," quoting the phrase used by SOX in section 404.

Regardless of the source of the control criteria, be it internally or externally imposed, there is value in using a systematic approach to the overall design of the security controls. ITA is a disciplined process that provides the method and defines the documentation necessary for successful technology designs. All of

the other architectures — data, technology, systems, or network — become subcomponents of the whole ITA approach. Sometimes the term *enterprise architecture* is used to define the "go to" or goal architecture. In reality, each of these subsets in an existing organization could have three architecture stages: the existing, transition, and target architectures.

The most important message is how to use the discipline of architecture as described in this book to organize and manage the design process whether you're designing from a blank slate or trying to fix a complex existing system. The process fits each of the architecture work areas from network design to data structures with only minor modification involving the required documentation.

Looking Forward

Later in this book, the seven essential elements of the security matrix are defined as the framework encompassing security controls. This framework is important because it helps define the outside limits for the security controls design work. You'll explore some of the limitations inherent within each area of concern.

Several chapters center on using the architectural process to focus on all of the principles and design tasks necessary to deal effectively with identity, authentication, and access controls relating to protecting any categories of applications, information, or data. The role of directory services and metafunctionality is examined, and you'll see how they can be designed to work together to provide the basis for links between identity and access control.

Toward the end of the book, you'll look at the value present in federated identity schemes and how they might be treated, as well as potential risks in going too far with federated identity in light of SOX oversight. The end describes a vision of the future perfect world in which privacy and confidentiality boundaries are respected and enforced by design and digital credentials can be trusted.

Several appendixes provide useful information and guidance for the process.

Blending Science and Art

At a very fundamental level, Sarbanes-Oxley is calling for the genteel merging of the science of accounting and auditing with the science and art of information systems design. If there were no computers or calculation machines of any type, all of the SOX controls would be relegated to the physical world of locks and keys, combinations, paper trails, and security guards. Because computers and applications and Internet access are integrated into so much of what is done today in business and private lives, stepping up of the controls in the

digital world is long past needed. It is easy to predict that SOX over time will prove to be just another in a long line of access control quality issues facing organizations. The time to meet the security controls challenge and lay the new digital control foundation is now.

That bridge to the design of desired state of access controls is what this book is about. The science and art of applying architecture principles will get you there.

Seeing the Whole Picture

Security controls must be dealt with in a complete context. You can't just check a box because you are using SSL to secure the data transmission and are requiring a user ID and password. Yes, those steps are necessary, but they're only two of many layers and dimensions that must be considered individually and collectively to achieve adequate control mechanisms over access and data. Applying a systematic method of ITA design principles and enforcement documentation is the way to succeed. The documents resulting from the ITA effort capture the requirements for the controls, provide the basis for implementation, facilitate operations and ongoing management, become input into any needed analysis or change process, and provide proof of due diligence during audits. When the ITA process relating to security controls is ongoing, it shows an expected level of due care.

Reaching a fundamental understanding of what ITA is and how to recognize it is necessary. Technology terms are often used inappropriately, creating confusion. This is often true of the use of the word *architecture* when applied in the context of IT. Some in the IT field, in sales pitches or design discussions, present something way less than architecture and call it architecture anyway. Others with a business operations focus or in management roles think they know what IT architecture is, although they cannot explain to you what it means to them or, more importantly, what benefits it can bring to their IT operations or in meeting the organization's business goals and objectives. What's often being passed off as architecture is more like IT confusion or a game of "my picture is better than your picture."

This book provides you with some valuable insights into what constitutes ITA. More important, it will help you learn how to systematize your thinking on the subject and become better able to properly document your organization's technology plans and designs. Using the process of ITA design for security controls will, within a short time period, help you and your organization achieve a bold and understandable architectural model for successfully designing for the currently critical security areas of identity management, access control, and authentication. The process provides a basis for creating adequate protection of private or protected information and data in your information systems designs and projects.

My own transition from a facilities management specialist working with hundreds of building architects and civil, mechanical, and electrical engineers on scores of construction projects over a 10-year period to an IT specialist made the concept of IT architecture easy to grasp but the details equally elusive. The effort and person-hours necessary to design and fully document an IT architecture supporting a complex heterogeneous enterprise scattered over a large geographical area with diverse lines of business and operational requirements is a daunting task. When it is divided into smaller building blocks or subcomponents, the job is much easier to envision and actually complete and implement during the build phase.

Document, Document, Document

Soon you'll see the documentation components required for successful ITA implementation of security controls in modern enterprises of all kinds that utilize computer information systems, networks, and data applications that do financial processing or house confidential information.

The order of doing the ITA design work is important. Just as buildings are rarely constructed from the roof down, when certain computer technology components are chosen that become foundations for follow-on components, the rest of the effort necessary for the design, documentation, and implementation all become easier to achieve within the overall systems environment one layer at a time. The foundation-first principle is truer in the technology field. There is a succession of thought that must follow a line of natural progression to develop the architecture from nothing for a new organization or from an "as-is" condition for one already invested with computer systems and applications to a new or desired vision state. The vision state or "to be" may also be called the target state or desired target or even target condition. You will see one path of this progression in Chapter 3 where the documentation process begins with business objectives and builds from there to successively include more detailed and often more complex documentation, each building on the documents that preceded its own development.

Seeing Caution Flags

All too often a CEO or CIO allows a single contractor or a mix of vendors to quickly decide what is in the best interest of the project or what best meets the company's needs in a given area of technology. This is as understandable as it is pitiful. The principal cause for this situation is the time pressure to get it done right now, which frequently gets in the way of getting it done right. Unfortunately, vendors rarely have time to sufficiently understand a client's business needs and are also reluctant to suggest a competing product as the best fit to solve a problem.

Companies on both sides of the contractor/contracting relationship rarely have sufficient time or all the in-house talent necessary to get every piece of the technology puzzle 100 percent correct in the specification or within the implementation process. "Correct" in this instance means performing to a standard as good as it can be, given the current technology available.

Shortcomings always exist in request-for-proposal specifications or in a project's management or within the implementation and delivery, hence the incredible forced popularity of the usually undesirable and expensive change-order process. Failure to apply a methodical design process is manifested in the worst situations where a technology consulting contract takes shape in only days or weeks and is given an expected delivery duration of 9 to 12 months, and after 3 years, the consultant still occupies a corner office. The company's comptroller is still writing or approving checks for cashing in a far-away bank. To add insult to injury, the original project scope is not finished yet and few if any of the original project deliverables perform as envisioned by the management group that first approved the project.

You can prevent this kind of scenario by having appropriate information technology architecture and an established process for information technology architecture design, changes, and redesign, and the necessary documentation. A repeatable ITA process is fundamental to preventing costly, even disastrous projects from wasting resources.

Increased Technical Complexity

Historical architecture models or starting frameworks such as those originally presented by J. A. Zachman in the *IBM Systems Journal* (Vol. 26, No. 3, 1987) are great at organizing both the questions that need answering and the array of perspectives required in considering the design views. However, they rarely provide the means to achieve the levels of detail really needed in a successful architecture design project. From the perspective of the interfaces, the earlier approaches are a great starting point, but all too often, they do not capture the multidimensional nature of the many relationships and flow-of-data interfaces required to make current applications work within the systems environment or complex interconnected networks and N-tier systems commonly in use today.

You and your organization are on the way to being better prepared to answer the question: How do you handle the issues of identity, authentication, and access control in your information technology environment to meet access control objectives? With the added emphasis today on compliance with government regulatory agencies' requirements to first provide accurate data to the agencies and the public, and with the groundswell of cases of identity theft in the morning news, appropriate access control strategies become critical to every computer environment.

Architecture Basics

After you explore basic ITA concepts in a general way, you'll examine a method for achieving the inclusion of architectural principles and appropriate documentation in your systems' design process. This is a design process that is both logical in approach, workable, and sustainable moving forward. The added benefit of using this approach is in having developed sets of documentation that flow naturally to uses in the operations environment. Once developed, these documents also take great strides toward the standardizing of daily IT systems operations.

Stepping Back

To see the concepts behind information systems architecture, first take a quick look outside the area of IT and computers at an example that applies a well-established architectural discipline to the design process: land-use planning and building construction. The field of land-use, zoning, and city or area planning works with architectural models or patterns on huge maps outlining where the various residential and specific-use areas will be placed, along with the density of construction in each of the specific-use areas. The locations for streets and water, sewer, gas and electric lines are well described and sized by engineers. Shopping areas, industrial zones, and green spaces are all placed on the map to create useful relationships, traffic flows, and use patterns.

To satisfy the political interest and at the same time accomplish the developer's objectives, various standard land-use design patterns are applied. These are transferred first to the maps and then later to the land itself during construction. In good land-development projects, a measure of creativity is applied as well to make the area aesthetically appealing to a particular target demographic.

After the land-use planners leave their work and move on to the next project, other professional disciplines such as civil engineers, building architects, and electrical and mechanical engineers become more involved in the architectural design process. Each engineering specialty in turn adds significantly to the collection of documentation and mounting details that help further determine the shape and look of the construction of buildings, the environment in which they will rest, and the infrastructure that will make it all work together as a connected working community.

Then interior designers and landscape architects and gardeners apply the finishing touches and further add to the beauty, usefulness, and utility of the structures and surrounding areas. Complementary colors and textures and just the right furnishings are added to the indoor and outdoor living spaces. A garden here, a few trees there, a well-placed shrub, flowers, topiary, outdoor furniture, and some outdoor play equipment are fixed into the individual yards to further advance the vision of quality living space.

Finally the most adaptable element is added to the implementation: the residents — the people that live, interact, and work there, making the system complete.

When you drive through a new subdivision, the architectural choices and styles become overwhelmingly evident even if you are not particularly attuned to the topic of architecture. Observers tend to say things like "drive past all the tick-tack houses until you come to the wrought-iron fence, and turn in where all the Victorian houses are." Although houses in a subdivision are not exactly the same, you can usually recognize them for their similar architectural styles. Theoretically, five separate houses could be designed and constructed to meet the exact same specific owner needs and requirements; contain precisely the same number, function, and size of rooms, doors, and windows; and include the equivalently useful fixtures, appliances, and equally desirable finishing elements and yet appear to be totally different from any of the other houses. In historical building architectural terms, descriptive names and styles are ascribed to the range of different homes: Victorian, Arts and Crafts, Postmodern, and Early Modern, for example. Each of these homes could be equally useful to the prospective owner in every respect, yet they could be strikingly different from one another visually and in their respective relationship to the environment and still be recognizable as belonging to its type.

Stepping Forward

Just like neighborhoods, houses, or building interiors, your enterprise's computer information systems architecture will take shape either by chance or by choice. The decision is yours.

Every neighborhood has a house that was built haphazardly and incrementally over time where nothing matches or fits the rest exactly right. You may have been to or even inside of places that are a true hodgepodge of pieces hammered together over time where nothing seems to go with anything else in any perceivable way. If that is how an observer would describe your company's computer system environment, you are really in need of the discipline of information systems architecture.

Process and Result

Architecture applied to design is fundamentally two things. First, it is a regimented process used to design or create something of value. A car, a house, a garden, or a computer system may each use an architectural process in the planning and design and enforce a method of assembly or construction that adheres to the features and appearance of the designer's vision. Second, the use of architects or the architectural process implies that it is intended to lead

to a qualitative result that can be readily recognized for what it is and as belonging to or as a recognizable member of its defined class by others knowledgeable enough to discern the difference. The resultant end product can be identified because it conforms to a defined pattern and set of standards.

When you think about applying a regimented process to information technology systems designs, the operative principle is control, actually a very high level of control derived from having a handle on a painstaking level of details. The complexity required to build a network and to place systems in it along with software and applications that function well for the end user works against achieving a high level of control in the early stages of the design process. That's mostly because getting to the level of detail needed is hard work — very hard work — and usually beyond the technical capability of any one person, even for a small-scale system. Recall that the building construction analogy alluded to the same issue. Building architects must work together with other engineering disciplines to work out all of the necessary details that are within the vision of the architect's objectives to create something new and distinctive but constrained by using currently available components and technology.

Applying Architecture to Legacy Systems

Information technology architecture improvement efforts and initiatives are frequently compounded, even confounded, by legacy systems. Legacy systems are the aged ones that are made up of older technology riding on sometimes clunky hardware that, unfortunately, end users and business processes use every day to keep the company running. Legacy systems and software impede progress because they are difficult to abandon and costly to replace. The organization that constantly postpones, delays, or ignores taking the steps to use and assigning the resources for an architectural team and process fails to achieve good design because they defer to tactical decision requirements over strategic planning. They often compound their own problems from having to deal with those costly and inefficient systems.

Legacy systems and existing applications are not exempt from regulatory oversight. The need to tighten security controls over existing systems and applications cannot be overlooked; otherwise, compliance audits will reveal the predicament.

Staffing the IT Architecture Design Team

ITA efforts require a high degree of commitment for success from the organization's top management. The right team of professionals must be assembled;

they have to understand the complexity of any legacy systems currently supporting the organization and the points where business processes and technology converge. Sponsors at the management level must be sure to appoint to the design team people who understand the target technologies and, most importantly, what is possible to achieve by using them.

The organization's business operations units will rely on the newly designed or reengineered systems to support their daily work. Representatives of those units must be included on the team to maintain the IT connection to the business. Their early participation makes the purposes for investing in and building the new or improved systems and application environment easier to attain.

Selecting the right reporting and accountability relationship for the information systems architecture team is perhaps the second most important executive decision. It is at least equal in magnitude to getting the right people on the team. If the objective is to make bold leaps into the latest technologies for reaching a goal of distinct and measurable competitive advantage in your organization's field of endeavor or your company's business against rivals, then having the team report to the chief information officer may not be the right choice. Most chief information officers and chief systems security officers today spend an inordinate amount of time reacting to issues brought about by daily operations and ever-increasing levels of security threats. All too often they are also required to meet these daily challenges with reduced staff rosters. Under these circumstances, a CIO could easily be both risk- and change-averse, and inclined to inappropriately tone down what a freethinking, empowered architecture team could propose.

Having the architecture team reporting to the highest level of management possible within the organization is perhaps the most desirable reporting structure. The chief executive officer who recognizes the potential competitive value of staying current with technology may well be the best guarantor of and accountability point for a truly empowered IT architecture team. Figure 1-1 illustrates a couple of the relationship choices you might make.

Today, in addition to the opportunity for the architecture team to improve systems for competitive advantage, there is the challenge of meeting regulatory compliance for security controls and system protective measures on state, national, and even international levels. The architecture process can also begin to design in security features to counter the liability risk facing every organization from system breaches leading to identity theft and compromises of privacy information.

So what should an information technology architecture team be charged with doing? What is their role? Why should any organization with significant capital outlay and operational expense for technology have such a team?

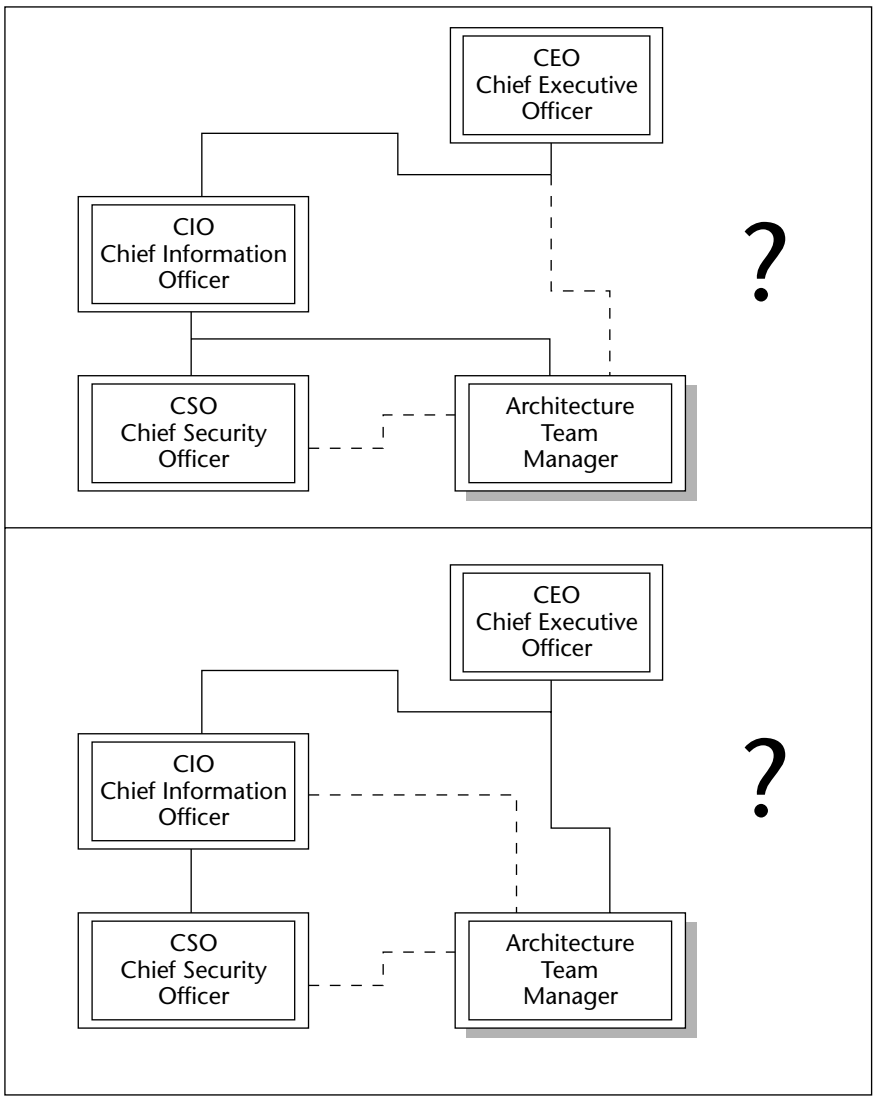

Figure 1-1 Carefully consider the reporting relationships for the architecture team manager.

Creating, Documenting, and Enforcing Architectural Design

There are five universal situations in which an information systems architecture team can greatly benefit an organization:

- A newly created organization that has no existing IT systems.
- A business where there is an investment in technology but management perceives that the technology is not serving its purpose very well, is not very efficient to use, and is too costly to operate, or the legacy systems are facing obsolescence.
- An organization in which internal parts are being fused to another part or when a whole company merges with another through consolidations or buyouts.
- An organization in which the existing investment in the IT systems is not providing the competitive advantage in the marketplace that could be gained from new systems or application improvements or replacement. (This is perhaps the highest strategic reason for using an information systems architecture team.)
- A business in which an objective evaluation of the existing systems clearly shows that the systems and applications as they exist do not provide for the levels of security controls necessary to meet compliance audits or an adequate defense against those who would do harm.

In all these cases, but possibly greatest in the last two examples, the team's goal is to apply their collective creativity and discipline to creating a system that be a measurable and lasting value for the organization.

Creating Value with Architecture

The design team will first create value by performing sometimes painful analysis of the existing situation with systems, applications, and business processes to create the documentation that describes what exists within the networks, systems, applications, and data stores. This first task is often the hardest part of the job because a lot of existing systems and applications were implemented over time and there's generally no roadmap or adequate documentation of "as built" design information.

In the analysis, the first question must always be this: Is this application, control, system, or software meeting the business objectives? And the second question follows up: Is it as good as it can be? Every application, every data store, every piece of hardware, and every interface requires examination and documentation attesting to the existing condition. The recipe for success is to categorize starting from each application. The end-user interface is where the business work product begins and ends. Architectural teams must approach their work from the end-user application perspective. Both the existing set of applications, or legacy if you prefer, and those features and capabilities desired in the vision that do not currently exist must become the focus and starting point of the architectural design process.

This application-first approach is necessary first to keep the spotlight where it belongs — on the end users and what the system does for them — and second, to facilitate the design team's getting a handle on what would otherwise be a very complex problem to document, understand, and analyze from any other perspective. Just as the accounting profession focuses on following and properly accounting for the flow of money, in the information technology architectural field, the approach to understanding and documenting (accounting for) the data systems design must focus on every one of the pathways that the data (information) takes as it is moved about and acted on to accomplish the organization's work.

For example, to describe the data paths for an e-mail application, you'd begin at the keyboard. The data flows include keyboard to CPU application, to network transport, over network to post office or SMTP (Simple Mail Transfer Protocol) transport send process, and so on. Along the way, every device, device interface, firewall, host, and security sector the data crosses must be captured, described, and documented in detail. Every point where one application passes data to another must be captured. Details of other processes that support the application, such as DNS (Domain Name System) host lookup to allow the e-mail to travel via SMTP over the Internet, must be included in the data paths documentation relating to e-mail. The bird's-eye view is from the perspective of the application. In the building construction design analogy, the details of the plumbing system's design and construction in effect follow the flow of the water. The details of the flows and controls that get hot water to the left faucet and cold water to the right one are the design focus.

The next phase of the analysis must examine the evidence to find the answer to the second question (is it as good as it can be?); determine where there would be benefit from a change in the hardware, software, applications, controls, or business processes; and place a value measure on making those proposed changes. This requires an end-to-end analysis of all of the interfaces and data flows that the system accomplishes to support the business process.

Once an objective measure is made of where changes or new additions need to be made, the team moves to the next phase: researching the scope of possibilities for making the system improvements. The results of exploring what is possible using the currently available technologies, tempered by the constraints that exist within the organization, become the catalyst or beginning bubble model for visualizing the first phase of the desired design.

Documenting for the Desired Design

The first of the two sets of documents represent what currently exists in the enterprise in detail. The second set of documents is the bubble model that represents the desired or target state. The entire discipline of information technology architecture must completely bridge the documentation gap between

these two states. It is theoretically the same as the building construction example if you said you have an existing state, a beautifully wooded 10 acres in the Keweenaw Peninsula of Michigan, and a fixed budget. Your desired state is to have a 2,000-square-foot log home on the property, along with a garage and a pole barn that blend into the forest. The buildings should be made mostly from on-site materials and must be built within the budget.

The documentation that allows moving from the existing state to the desired state is brought about by the construction architecture creative design, a process where design concepts are expressed in detailed drawings and specification documents. The building example may be theoretically the same, but in most complex enterprises and technology environments, IT architecture is much more multifarious in nature and requires significantly more documentation and greater detail than is found in sets of building construction documentation.

Information technology architecture requires more than a picture or a diagram of hosts and devices placed in a network to achieve the affirmed goals of its practice in IT systems design and implementation. The architecture team must achieve a level of documentation that leaves no doubt in the mind of the in-house or contracted applications developer or implementer what the systems are to look like, how the application will be developed, how everything works together, and what all the interfaces are. It must leave no gray areas as to how the systems are to be operated, maintained, and when necessary, modified.

The documentation must be complete enough to answer most any question the operations personnel charged with supporting the systems and applications might have. The new developer must know exactly how to fit the new application into the existing environment without creating damage to existing systems or proposing new, alien, or costly-to-support alternative solutions to what was intended. Sure, diagrams depicting the infrastructure are needed, but so are all of the text documents detailed in Chapter 3. Diagrams without the complete sets of supporting documentation are of little value. Collectively, the necessary diagrams, recognition of the policy enforcement zones, and the documentation described in Chapter 3 facilitate and constitute the body of information that is systems architecture.

Enforcing Design Vision through Documentation

In large companies, modern fast-moving enterprises, and organizations where information technology systems and supporting operations are dispersed or where authority is not centralized, enforcement of information systems architecture is a daunting task. Often the accommodating IT staffs, while being helpful in trying to do something better-quicker-cheaper, violate the intended systems architecture, causing increased security risk and adding unnecessary cost to the support phase of an application's life cycle.

Enforcement of completed information technology architecture designs and documentation in any organizations must find its way into the personnel/job descriptions of everyone who plays a role in implementation, modification, operation, maintenance, or application development. In other words, everybody in the IT department, including management, must have within his job descriptions a firm performance link to complying with and enforcing architecture, policy, and standards.

No Legal Enforcement

You find a level of legal enforcement in the field of building construction. States have construction code commissions that establish rules and regulations from laws that control the regulatory oversight of home and building construction. It comes in two modes. First are the building codes, such as BOCA, adopted by local charters and laws and enforced by a body of government trade or general construction code inspectors. The second mode is achieved by licensing home builders, electricians, plumbers, and heating and ventilating contractors, where failure to perform installations to code standards could lead to loss of license. Even though the IT field has, through notable software and hardware vendors such as Cisco, Microsoft, and Novell, offered training and certification, there's no assurance that your design and implementation objectives will be met even when done by certified professionals. Having CISSP-certified staff does not always equate to a system as secure as they should or could be. (CISSP stands for Certified Information Systems Security Professional.)

This places the burden on an organization's management to protect itself by developing a quality in-house practice of information technology systems architecture or by contracting with consulting firms that have established practices with a track record of success. For an organization that cannot afford either option, there is at least a conceptual alternative that has yet to catch on in the industry: third-party plan review. This means that before a vendor proposal is accepted for implementation, a disinterested but qualified third party reviews the details of the implementation to help ensure that the proposal at least meets the objectives. Qualitative third-party design review can help determine if what is proposed by vendors for purchase is at least current technology and efficient if not state-of-the-art for similar implementations.

For those organizations new to the concepts and discipline of information systems architecture as a tool to rationalize what can otherwise become an out-of-control spiral of technology and costs, this is the prime means to get a grasp on expenses and increase the benefit derived from the technology. For those entities that are already heavily investing in the practice, a renewed focus can bring ever-smaller elements under the purview of the process to solve current challenges.

Security Issues Always in Sight

Current design challenges frequently revolve around security issues including protection of privacy, protection of financial data, establishing accountability of access, and sufficiency of the audit capability. The publicity surrounding these topics is driven in part by the Sarbanes-Oxley legislation requiring improved controls and accountability within public companies. The comprehensive solutions to these issues require a higher level of architectural discipline in the design process and operational practices than many of today's information technology systems have.

Keep in mind that this is a complex area often requiring focus on microscopic details that apply to abstract layers of the systems and interfaces. Concentrating on one subset of the bigger picture, such as the security, and approaching design elements from an application perspective makes success possible. That is, resolving to make your applications secure one application at a time will lead to a secure enterprise. Each time an approach works to secure an application, it has the potential to become the pattern for the next round of applications. For example, setting up identity services for the new applications potentially allows retrofitting of the legacy application to use the same service. Establishing the controls inherent in a security architecture design from a priority list one application at a time is the most workable tactic. Using such a methodical approach allows the patterns of the solution to emerge and be leveraged in the subsequent work.

Chapter 2 discusses the individual elements of data and privacy protection that must be controllable for access and accountability. As you read through it, keep in mind that each of the nine elements of data or privacy protection presented there must be evaluated as to whether it should be controlled for access within the circumstances of the data use in your organization. If the answer is yes, then the next question becomes how you can design to accomplish that required control within your architecture at all appropriate levels. Any system's security architecture design will be judged, audited, and qualitatively ranked on how well it can control each of those elements.

Summary

In addition to HIPAA, Gramm-Leach-Bliley, state privacy protection laws, and regulatory requirements imposed in doing business internationally, SOX compliance is just one more reason to use a comprehensive architectural design team and process to create new or improve your current IT systems. IT systems are already complicated, and adding spotty upgrades and patches simply intensifies the complexity without necessarily increasing the security

protections. The access controls that should be designed to meet requirements for regulatory compliance may turn out to be the key defense contributing to an organization's very survival from the next big IT worm or hack attack.

The process of formalizing the effort to turn business needs into requirements and requirements into new systems and hardware has value and can pay dividends to the firms willing to trade some legacy systems, applications, and controls for ones designed to meet modern operational and control challenges.