Executive UPDATE

CUTTER CONSORTIUM
Access to the Experts

BUSINESS & ENTERPRISE ARCHITECTURE

Business Architecture's Role in Crisis, Risk, and Compliance Management

by William Ulrich, Fellow, Cutter Consortium

Every business must deal with crisis, risk, and compliance challenges. Teams chartered with addressing these challenges are often split across business units and regions, which fragments crisis, risk, and compliance management efforts. Business unit silos and related complexities obscure ecosystem transparency, which in turn constrain an organization's ability to identify risks, assure compliance, and prevent and disarm crises. Business architecture delivers business ecosystem transparency as a basis for improving a business's ability to collectively address challenges related to crisis, risk, and compliance. This *Executive Update* outlines the role of business architecture in crisis, risk, and compliance management.[1]

Defining Crisis, Risk, and Compliance

Establishing a shared understanding of crisis, risk, and compliance management is the first step toward understanding business architecture's role in improving how organizations deliver on each of these disciplines. Consider the following definitions:[2]

- **Crisis** — an unstable or crucial time, or state of affairs, in which a decisive change is impending; especially one with the distinct possibility of a highly undesirable outcome

- **Crisis management** — the ability to proactively plan for and respond to disruptive and unexpected events that threaten to harm the organization, its stakeholders, or the public

[1] Author's note: "governance, risk, and compliance" (GRC) is a common industry term but we do not use it here because the topic aligns crisis, risk, and compliance, whereas governance is a unique subject.

[2] Sourced primarily from BusinessDictionary.com.

- **Risk** — a situation involving exposure to danger
- **Risk management** — the ability to identify, assess, control, avoid, minimize, and eliminate unacceptable risks
- **Compliance** — confirmation that the doer of an action or supplier of a product conforms to accepted practices, legislation, rules, regulations, specified standards, and contract terms
- **Compliance management** — the ability to identify, assess, and assure that a business conforms to accepted practices, legislation, rules, regulations, specified standards, and contract terms

While many businesses tend to have unique business teams dealing with each of these disciplines, the overall ability of a business to identify and manage compliance and risks, and to prevent and respond to crises, have a great deal in common. In other words, crisis, risk, and compliance management are highly intertwined disciplines.

For example, organizations identify weaknesses, threats, and related impacts as a basis for mitigating risks and future crises. They also seek to achieve compliance to avoid legislative, audit, and oversight violations and related disruptions that could stem from these violations. Each of these disciplines relies on varying degrees of business transparency as a basis for prevention and remediation, with a focus on nullifying customer, partner, public, employee, and general business impacts.

Crisis management is a good starting point for examining common ways to improve a business's collective ability to exercise these disciplines because avoiding and responding to crises requires highlighting and mitigating risks and assuring overall compliance.

Crisis Management in the News

In 2016, Wells Fargo discovered that as many as 2.1 million people were the subject of problematic sales practices where unauthorized accounts were created for these individuals. The following series of headlines, which ran from September 2016 through March 2017, help illustrate this story:

- "5,300 Wells Fargo employees fired over 2 million phony accounts," 9 September 2016
- "Wells Fargo Struggling in Aftermath of Fraud Scandal," 13 January 2017
- "Wells Fargo is closing over 400 bank branches," 13 January 2017
- "Wells Fargo says more customers could be affected by sales scandal," 1 March 2017
- "Wells Fargo credit card applications plunge 55 percent in February," 20 March 2017

Wells Fargo’s CEO indicated in an article dated 17 March 2017 that the company “is looking as far back as 2009 to figure out how many unauthorized accounts were created.” The CEO was further cited as saying, “I will describe it as much more complicated than anyone could have imagined. But that’s not an excuse. It’s going to take a few months to figure out. But I will assure we will remediate all those customers.”

When crisis hits, it hits hard, and if an organization lacks certain levels of business transparency, recovery from that crisis can be a long, painful, and even very public process. Heading off crises requires identifying and mitigating risks and ensuring compliance, creating a triumvirate of interrelated disciplines that demand total ecosystem transparency.

Total Ecosystem Transparency: Managing Crisis, Risk, and Compliance

In a crisis, executives require rapid cause-and-effect analysis. Unfortunately, this type of analysis is often cobbled together in haphazard ways across disparate, uncoordinated business units. Within this context, no one area can see the whole picture, which means, for example, that upstream impacts are shrouded from downstream business units. In some cases, the actions or impacts of a business partner further complicate cause-and-effect analysis. And in almost all cases, the lack of a defined business vocabulary across business units means that tracing the evolution, location, and state of a contract, customer, product, asset, investment, account, or other critical business perspective is at best fleeting for any given area and fully shrouded from the business as a whole.

Business ecosystem transparency facilitates risk identification and avoidance, regulatory and related policy compliance, and rapid cause-and-effect analysis in a crisis. The business ecosystem is an important concept here because it establishes the scope and boundaries of a business that is not fully reliant on business unit silos. As defined in *A Guide to the Business Architecture Body of Knowledge® (BIZBOK® Guide)*, a business ecosystem is “one or more legal entities, in whole or in part, that exist as an integrated community of individuals and assets, or aggregations thereof, interacting as a cohesive whole toward a common mission or purpose.”

The above ecosystem definition helps when defining business boundaries, which seldom begin and end with a single legal entity. Consider, for example, a company that outsources certain capabilities, such as Legal Proceedings Management, Asset Definition, Shipment Management, Feedback Management, Payment Determination, and Human Resource Management, all of which are key to the company’s success. Whether insourced or outsourced, these capabilities, which define “what” a business does, are part of the business ecosystem because they are essential to ensuring that a given business is a viable, functioning entity.

Lack of Business Transparency Fosters Crises, Risks, and Noncompliance

Crisis scenarios tend to trigger reactive, versus proactive, responses. Underlying these reactive response tendencies are piecemeal, siloed approaches to compliance and risk management. For example, risk management at large, multidivisional companies can lack holistic perspectives of risk-related impacts across customers, partners, products, markets, and related focal points. There is no concept of ecosystem-wide risk aggregation across these business perspectives or related business units. As a result, what appears to be in compliance within a given business unit may receive a failing score in aggregate across multiple business units.

Consider a financial services firm with multiple divisions and multiple business units within each of those divisions. Each division and related business unit would be responsible for managing multiple accounts, products, funds, and, depending on its business model, policies for insuring wealth. Individual business units would have instances of common capabilities, such as account management, fund management, customer management, product management, transaction management, and payment management. Figure 1 illustrates an example of such a business scenario.

Figure 1 highlights that each business unit has a siloed view of its accounts, customers, products, and other focal points. In this scenario, each business unit would work under the assumption that it is in full compliance with policies and regulations and that it has adequately identified and mitigated risks. Each business unit has its own crisis management plan. On a case-by-case basis, each business unit would score very well in terms of crisis prevention, risk management, and compliance. In all likelihood, however, the exact opposite is true.

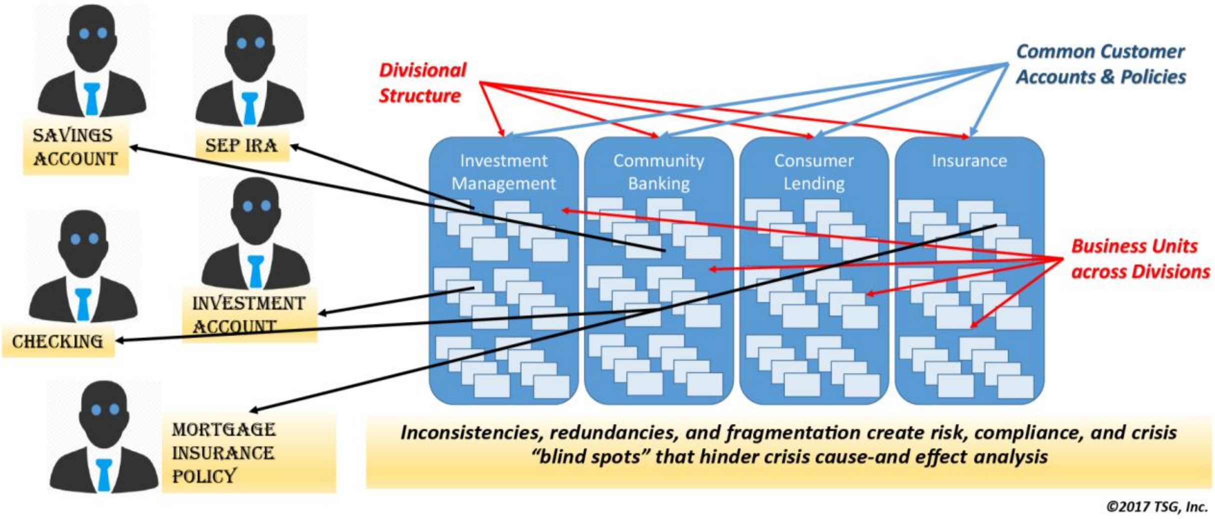
SAVINGS ACCOUNT
SEP IRA
CHECKING
INVESTMENT ACCOUNT
MORTGAGE INSURANCE POLICY
Divisional Structure
Common Customer Accounts & Policies
Investment Management
Community Banking
Consumer Lending
Insurance
Business Units across Divisions
Inconsistencies, redundancies, and fragmentation create risk, compliance, and crisis "blind spots" that hinder crisis cause-and effect analysis
©2017 TSG, Inc.

Figure 1 — Complexity and redundancy across business units creates crisis "blind spots."

Cross-business-unit complexities, redundancies, and fragmented business views have blinded the business as a whole to potential risks, overall compliance, and, most important, the ability to plan for and mitigate risk. Figure 1 highlights the fact that each business unit sees the customer as its own customer, without understanding that a given customer may have multiple accounts, funds, and policies with the business as a whole. The customer sees one company, but the business collectively sees that customer as many entities.

Consider a scenario where a customer defaults on a mortgage. That same customer holds many other accounts, investments, and policies. In addition, that same customer comes back to the institution to get another loan from an unrelated business unit, despite the fact that the originating business unit marked that customer as a credit risk. Now multiply this scenario by millions of customers, accounts, business partners, products, payments, decisions, and a host of other business perspectives.

The institution's ability to perform aggregated risk analysis, ensure compliance, and prepare for and react to crises, is dramatically impaired by these siloed business perspectives; silos that include functionally and regionally aligned business units. Executives can stress cross-business cooperation, but this is a piecemeal approach that veers more toward wishful thinking than aggregated crisis, risk, and compliance management.

Business fragmentation is not uncommon. In fact, it is the norm across numerous industries worldwide. Businesses have historically pushed crisis, risk, and compliance management to individual business units. In many cases, a centralized risk management team is in place along with corporate audit and crisis management teams. But these teams have no more visibility across a fragmented ecosystem than would any other business unit, which means that they can establish and push out policies, but there is no way to verify compliance in an opaque ecosystem.

How can multibillion-dollar, multidivisional corporations take these risks? Why would oversight agencies, auditors, and executive governance structures ignore these risks? Are executives aware of the risks related to this lack of transparency and the impacts on the business? If a business is not familiar with the benefits of and the capacity to establish ecosystem transparency, then perhaps there is simply a sense that there is nothing that can be done. But this is not the case.

Business Architecture: Delivering Business Ecosystem Transparency

Business architecture provides the transparency needed to proactively avoid crises through risk and compliance management — and to respond in kind when crises do arise. This means, for example, that a business will view a customer just as the customer views the business: through a single lens with multiple accounts, policies, and investments. Customer risk and account risk management become

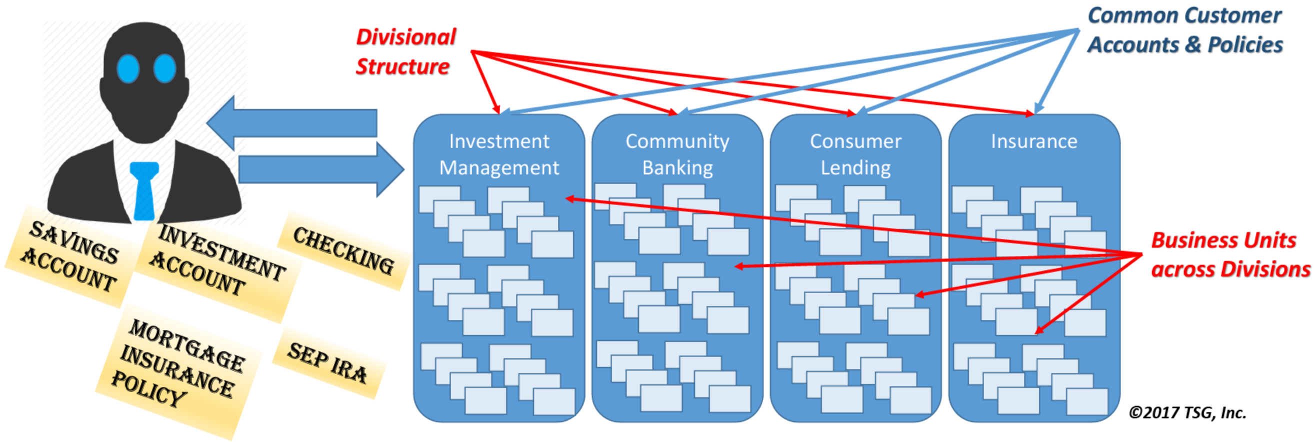

Figure 2 — Business-viewing customer: shared interests through a common lens.

shared capabilities that consider the customer in totality and not through many business unit silos. Figure 2 highlights this single-view perspective on customer and related interests.

A well-articulated business architecture provides rapid insight into which customers are aligned to certain accounts and agreements, how customers are linked to other customers and third parties, associations among accounts and agreements, and related business unit impacts. Business architecture highlights where blind spots exist, pinpoints impacts on the business from an ecosystem-wide perspective, and provides insights into resolving risk, compliance, and related factors.

Business architecture delivers the business transparency to deliver these insights by articulating a common set of rationalized, cross-business perspectives on capabilities, stakeholders, value delivery, and information. Leveraging this baseline business architecture perspective, planning and execution teams can selectively view the business from a variety of business unit, business policy, strategic planning, initiative investment, and product perspectives. These perspectives, in turn, are applied to assess and manage crises, risks, and compliance for the business as a whole.

Consider, for example, the policy and regulatory compliance perspective shown in Figure 3. A well-articulated business architecture would have business-wide capability definitions mapped out along with the business units that have or exercise those capabilities. When viewed through a policy compliance lens, regulatory, audit, and compliance teams can quickly assess policy impacts, points of risk, and related focal points for crisis management. A business may choose to drill down to a product, initiative, investment, or numerous other perspectives.

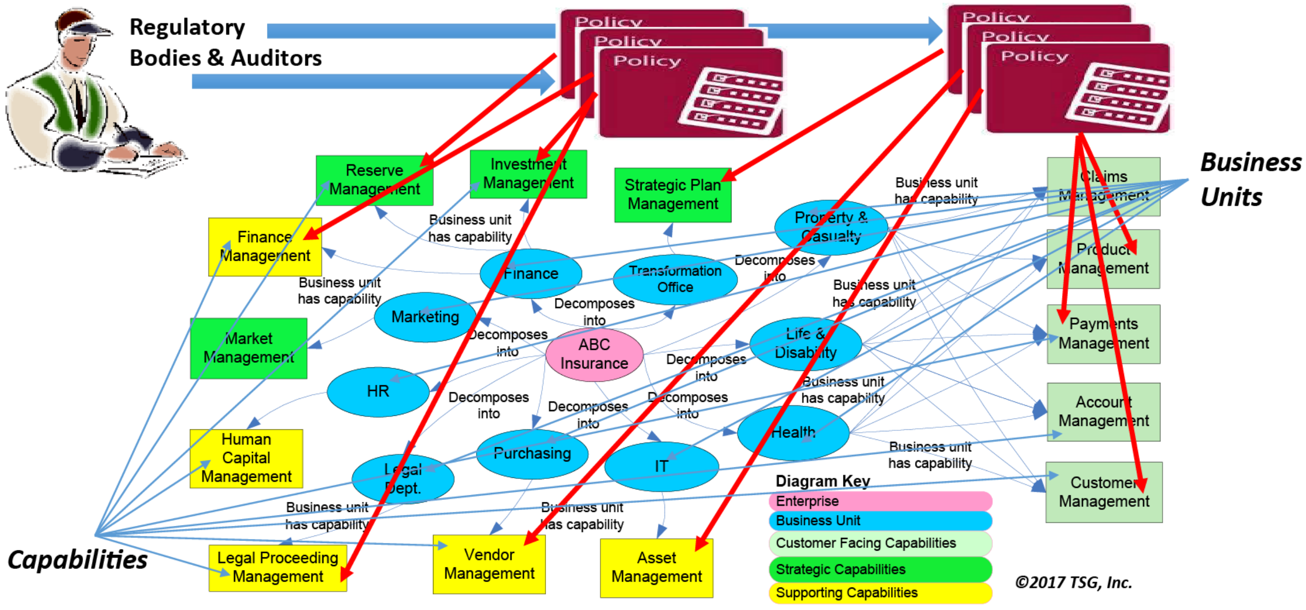

Figure 3 — Business policy and compliance impacts on business units and capabilities.

If a business has this level of policy compliance understanding and insight, crisis and risk management becomes a matter of providing this information to any team that requires it, and this could extend well beyond a given crisis management or audit team, ensuring that policy compliance is built into the fabric of the business from planning through deployment.

Consider the value of having the transparency shown in Figures 2 and 3 in reference to the challenges faced by Wells Fargo as outlined at the outset of this *Update*. The business would be able to trace an account to a customer and a customer back to all accounts and related impacts. This could also include customer relationships to policies, investments, partners, assets, or even other customers. The insights become second nature, not multiyear investments across many dozens of business units.

Business-Driven Crisis, Risk, and Compliance Solutions for IT Architecture

At this point, one would presuppose that any degree of crisis, risk, and compliance management would certainly target or at least touch upon information systems as well as drive investments in those systems. The multidimensional transparency delivered by business architecture extends into the IT architecture domain. Capabilities, value delivery, information, and business unit perspectives may be associated with the information systems and wealth of other technologies that automate capabilities and related aspects of business architecture. As such, an investment in those systems should be viewed through the business

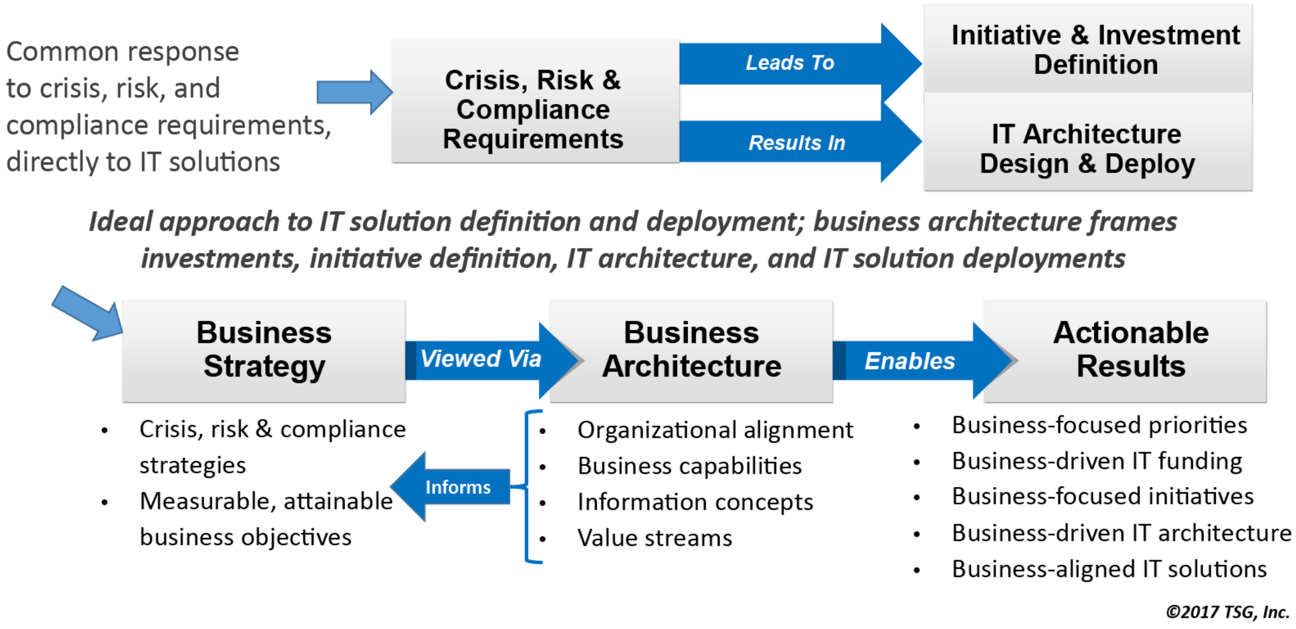
Common response to crisis, risk, and compliance requirements, directly to IT solutions
Crisis, Risk & Compliance Requirements
Leads To
Results In
Initiative & Investment Definition
IT Architecture Design & Deploy
Ideal approach to IT solution definition and deployment; business architecture frames investments, initiative definition, IT architecture, and IT solution deployments
Business Strategy
Viewed Via
Business Architecture
Enables
Actionable Results
Crisis, risk & compliance strategies
Measurable, attainable business objectives
Informs
Organizational alignment
Business capabilities
Information concepts
Value streams
Business-focused priorities
Business-driven IT funding
Business-focused initiatives
Business-driven IT architecture
Business-aligned IT solutions
©2017 TSG, Inc.

Figure 4 — Business architecture drives IT investments.

architecture lens to assess general business impacts as well as ideal options for furthering crisis, risk, and compliance management.

The top portion of Figure 4 depicts how most businesses pursue crisis, risk, and compliance management. A given business unit receives a request from a compliance, risk, or audit group and invests in siloed, redundant information systems to address the issue(s) at hand. The previous challenges associated with siloed views of a business and related constraints they place on aggregated crisis, risk, and compliance management spill over to IT investments.

The ideal approach is shown across the bottom portion of Figure 4, where crisis, risk, and compliance strategies are viewed through the lens of business architecture, which in turn is used to articulate updates to existing information systems or specifications for a more applicable set of systems. The key aspect of business architecture that focuses IT planning and deployment is the capability.

Capability-based planning offers a shared perspective for focusing IT investments on stakeholder value delivery, information alignment, and business unit synchronization. When capability-based planning is engaged, the many tens or hundreds of millions of dollars in IT investments may be redirected from a siloed, piecemeal, and highly limited solution deployment approach to a more holistic planning and investment perspective to enabling crisis, risk, and compliance management.

Leveraging Business Architecture for Crisis, Risk and Compliance: Call to Action

How should organizations move forward to leverage business architecture for crisis, risk, and compliance management? Here are some steps to pursue:

1. Determine your organization's business architecture maturity using a standard approach to business architecture maturity analysis.
2. Establish business architecture outside of a given business unit or IT group. This will provide transparency across siloed business perspectives that are in place today.
3. Educate relevant teams and executives on using business architecture for crisis, risk, and compliance management.
4. Outline steps for articulating your business architecture, with a focus on establishing a high-level, cross-business baseline, coupled with policy and stakeholder perspectives.
5. As the business architecture is established, begin to link it to the IT architecture as a basis for business-driven/IT transformation planning and investment.

Hopefully these steps will help your organization move forward with using business architecture for crisis, risk, and compliance management. One added element of this is that business architecture provides the basis to rethink how a business delivers stakeholder value. The transparency business architecture provides not only enables innovation teams to rethink how they address crisis, risk, and compliance management, but generally enables a business overall to envision and realize innovative thinking through perspectives that were previously hidden from line of sight.

About the Author

William M. Ulrich is a Fellow of Cutter Consortium's [Business & Enterprise Architecture] practice and President of TSG, Inc. Specializing in business and IT planning and transformation strategies, he has more than 35 years' experience in the business-IT management consulting field. Mr. Ulrich serves as strategic advisor and mentor on business-IT transformation initiatives and also serves as a workshop leader to businesses on a wide range of business-IT transformation topics. He has the unique ability to cross business and IT boundaries to facilitate and streamline business-IT transformation strategies, and his workshops on business-IT architecture transformation have been widely attended by organizations worldwide.

Mr. Ulrich is the cofounder and President of the Business Architecture Guild, Cochair of the OMG Architecture-Driven Modernization Task Force, and cofounder and Partner at Business Architecture Associates, Inc. Previously, he served in a senior management capacity at KPMG, including as Director of Reengineering Strategies, prior to leaving and forming his own company in 1990. Mr. Ulrich's work has been the basis for business and IT architecture transformation projects worldwide. Past clients include a wide range of large-scale corporations and government agencies worldwide.

Mr. Ulrich is a pioneer in the evolution of the practice and discipline of business architecture. As an originating author of A Guide to the Business Architecture Body of Knowledge® (BIZBOK® Guide), *he played a pivotal role in framing the now generally accepted approach to business architecture. He is a Certified Business Architect® (CBA®) and continues to play a role in formalizing industry standards around the practice.*

As developer of The Systems Redevelopment Methodology (TSRM/USRM), Mr. Ulrich defined many of the standards used in systems modernization within today's IT industry. He has also helped hundreds of organizations capitalize on knowledge built into their existing systems. A forerunner in the IT transformation industry, Mr. Ulrich was on the 1980 alpha test team for the first commercially available systems redevelopment tool and was instrumental in the development of the application reengineering and reverse engineering papers for IBM's Guide Project.

Mr. Ulrich has also served on the faculty of Northeastern Illinois University and facilitated numerous workshops, including sessions for SEI. He has lectured internationally to thousands of business and IT professionals and has testified as an expert witness on the use of IP within the computer field. Mr. Ulrich continues to serve as a software forensic and litigation support expert in technology-related cases. In 2005, he was awarded the Keeping America Strong Award by Rear Admiral Kevin F. Delaney (Ret.).

Mr. Ulrich has authored hundreds of articles appearing in major publications and journals. He is coauthor of Business Architecture: The Art and Practice of Business Transformation, Information Systems Transformation: Architecture-Driven Modernization Case Studies*, and* Legacy Systems: Transformation Strategies*. He can be reached at wulrich@cutter.com.*