82-01-70.1 Controlling Major Systems Integration Projects
Steve Mar

Payoff
IS management and users are taking advantage of such relatively new technologies as local area networks, client/servers, and distributed computer environments to create innovative strategies for systems integration. The information security specialist can play a key role in designing controls for systems integration projects only if he or she understands how these new technologies can be used to achieve the objectives of the integration project. This article examines the issues and risks of major systems integration projects, effective control designs for these projects, the impact of new technologies, and the effect of business decisions on the project. The article reviews strategies for systems integration, provides guidelines to design information security for new technologies, and suggests a model for the information security specialist to follow when developing controls.

Problems Addressed
Most problems that arise during the design and development of major systems integration projects can be resolved without significant impact to the project budget and schedule. However, an increasing number of these projects encounter problems that are difficult to control. Such new technologies as local area networks (LANs), client/servers, and Distributed Computer Environments increase the complexity and level of challenge to the systems integrator.

An integration project can encounter control problems for a variety of reasons, including:

- Poor planning and design.
- Lack of project leadership and understanding of requirements.
- Lack of controls and standards.
- Inadequate technology.
- Inability of user, management, and developer groups to work together.
- Incorrect design of information and data structures.
- Underestimation of the time required to convert systems and provide adequate documentation.
- Cost, funding, and accounting problems.
- Change in project direction, focus or management after the project has begun.
- Unqualified or inexperienced project team members.

In one case, for example, a health care provider was forced to write off several million dollars of development costs because of a failed integration project. The project had attempted to link field office processing, claims information and other customer functions
such as eligibility. The integration effort, which lasted several years, encountered problems with testing procedures, implementation of new technologies, and personnel problems.

The information security specialist plays an important role in the design and development of both project and security controls. The security specialist must be able to advise IS management on both traditional control issues and on the control problems and solutions involving LAN, client/server, UNIX, and other more advanced technologies. If security personnel are unable to contribute because of lack of in-depth knowledge of such technologies, integration projects are much more likely to be implemented without effective controls.

This article addresses the question of why such failures occur during large systems integration projects, discusses ways to prevent them, and provides guidelines for the information security specialist to use in assisting systems development management.

**Systems Integration Problems**

Problems in systems integration projects can be grouped by three kinds of factors: human, technical, and financial.

**Human Factors**

Human factors that may lead to problems in systems integration projects include:

- Lack of user group participation in the design and development process.
- Faulty coordination between users, developers, and management.
- Inadequate project leadership.
- Lack of top management focus and support.
- Lack of training.

For example, a large holding company purchased a number of different business product lines, including entertainment and publishing. The entertainment company did not have any systems experience and its users were not given adequate training. This led to major problems in converting, installing, integrating, and using the system. The publishing company, on the other hand, had an existing production system that worked extremely well. The publisher's management refused to use the integrated system, which has resulted in reporting inaccuracies at many levels.

**Technical Factors**

A number of technical problems can cause the systems integration project to run into trouble:

- Lack of reliable and accurate data files.
- Poor hardware and software capabilities.
- Misapplication of small online data base systems to handle extensive transaction volumes and updates.
- Lack of experience in new technologies used to develop the system.
For example, a brokerage firm ordered and planned to install a new UNIX system that would integrate its existing customer data base with a regulatory reporting data base. However, after several unsuccessful attempts at integrating the applications with the UNIX platform, management cancelled the project because the technology proved to be too unreliable and was unable to process the required volume of trading system transactions.

**Financial Factors**

Financial factors that create problems in major systems integration projects may include:

- Lack of financial control over the project process.
- Funding limitations.
- Lack of financial reporting and accountability.
- Cost overruns due to poor planning, contract disputes, and other commitments by vendors.

For example, a public utility selected a specific software vendor after a review of several vendors in accordance with its Request For Proposal process. Unfortunately, the software company ran into cash flow problems, which resulted in a slow down in system development. The resulting delay caused the utility to lose certain competitive advantages that would have resulted from timely completion of the project.

**System Integration Control Requirements**

The information security specialist should review three levels of controls:

- **General Business Controls.** These controls include development team qualifications, business reasons for the integration, business resumption, change controls, network controls, and access controls.

- **Application Controls.** These controls include input edit controls, communication controls, documentation controls, user controls, acceptance testing controls, processing controls, and output controls.

- **Project Controls.** These controls include budgets, schedules, performance measures, and project management.

The information security specialist should determine the types of controls to be implemented for the integration project. The necessary controls can be identified by conducting a risk assessment.

The next two sections discuss general business and application controls in detail. Project controls are beyond the scope of this article.

**General Business Controls**

A key factor influencing the risk assessment is the business reason for the systems integration project. Management would already have considered certain economic, product, customer, and operational factors in deciding to move ahead with the systems integration project. The security specialist should evaluate why management has decided to proceed with this project and determine what general business risks may need to be addressed. Exhibit 1 illustrates these risks and possible control concerns.
## Risks and Control Concerns Associated with Business Reasons for Systems Integration

<table>
<thead>
<tr>
<th>Business Reasons</th>
<th>Risk Issues</th>
<th>Control Concerns</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mergers and Acquisitions</td>
<td>- Business culture or management conflicts</td>
<td>- Inability to agree on general controls</td>
</tr>
<tr>
<td></td>
<td>- Loss of experienced management and staff</td>
<td>- Increased potential for operating errors and mistakes</td>
</tr>
<tr>
<td></td>
<td>- Lack of long-term investment</td>
<td>- No commitment to maintenance or upgrades</td>
</tr>
<tr>
<td></td>
<td>- Change in strategic direction and focus</td>
<td>- Lack of commitment to controls and direction</td>
</tr>
<tr>
<td>Corporate Downsizing</td>
<td>- Decrease in staff morale</td>
<td>- Employee fraud or lack of motivation</td>
</tr>
<tr>
<td></td>
<td>- Loss of loyalty</td>
<td>- Disregard for rules and controls</td>
</tr>
<tr>
<td></td>
<td>- Increased work load for remaining personnel</td>
<td>- Bypassing controls to get more work done</td>
</tr>
<tr>
<td>Outsourcing</td>
<td>- Loss of influence over development process</td>
<td>- Users install and create their own applications</td>
</tr>
<tr>
<td></td>
<td>- Inability to respond to market competition or develop new products</td>
<td>- Data integrity and reliability problems</td>
</tr>
<tr>
<td>User-Driver Integration Requirements</td>
<td>- Lack of technical experience</td>
<td>- Misapplication of technical control features</td>
</tr>
<tr>
<td></td>
<td>- Lack of user controls awareness</td>
<td>- Lack of support for controls by users</td>
</tr>
<tr>
<td>Improved Management Reporting</td>
<td>- Users create ad hoc reports without controls</td>
<td>- Duplication of effort</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Unreliable reports</td>
</tr>
<tr>
<td>Hardware and Software Cost Reduction</td>
<td>- Integration of systems without a central data base</td>
<td>- Data integrity problems</td>
</tr>
<tr>
<td></td>
<td>- Development of applications without network controls</td>
<td>- Network controls not implemented or given priority</td>
</tr>
</tbody>
</table>

Certain risks are inherent in the general business operations and information process. The information security specialist should assess the following control areas to determine the controls that should be implemented during development:

- Experience and qualifications of team members to ensure that they understand the importance of controls and can implement them correctly.
- Ability of the organization to continue processing in the event of a disaster.
- Testing of the recovery process to ensure it works as planned.
· Ensuring that updates to applications are appropriately designed, tested, and implemented.

· Ensuring that network controls are in place to route messages to the correct users.

· Maintenance of the confidentiality of messages during network transmission.

· Ensuring that the network remains stable and available to users.

· Implementing access controls to ensure that only authorized users are allowed on the system.

· Establishing procedures to determine when and how to remove users from the system.

**Application Controls**

When the project team begins to focus on the application controls for the system integration project, the information security specialist should assess the application risks and controls. If the new systems integration project relies on the existing mainframe system and operating environment, the information security specialist can evaluate or rely on existing mainframe controls such as IBM's Resource Access Control Facility or Computer Associates' CA-Top Secret for access control.

If open systems architectures are being implemented, a different approach to system and application control may be required. For example, workstation and LAN-based systems distribute information processing closer to the user and, in turn, require that users accept greater control responsibilities and oversight. The central data processing facility or computer center can no longer continue to provide certain application control services.

For example, when using Novell NetWare as the LAN file server and network interface, the information security specialist must know what version of NetWare will be installed for the systems integration project because different versions of NetWare provide different security features.

**Assessing Systems Integration Strategies**

Organizations use a variety of integration strategies to meet their business requirements. This section describes five integration strategies and demonstrates how these strategies affect the design of controls.

**Strategy 1: Full Integration**

This approach takes all existing systems and integrates them into a single, unified system. In one example, a manufacturing company decided to integrate its order entry, sales, and general ledger applications. Each system ran on a different platform and required different access methods. Screens did not look the same, and function keys did not operate the same. As a result, users made many mistakes in entering and retrieving information.

A consulting firm was contracted to design and fully integrate all the procedures and products on a single system. The consulting firm developed a new sales application to manage sales units, assign accounts, report expenses, review orders, and manage territory sales data. Information was made available in a database for both general ledger and management reports.

This is the best approach for this manufacturing organization, because it allows all the applications to be installed and maintained on a single system. The information security specialist was able to assist and develop a new set of comprehensive system controls rather
than update existing change procedures and controls. As noted, it is more cost-effective to design and install controls during the integration project than after the new system has been installed. However, this strategy requires a great deal of time and effort, senior management support, and a significant financial investment. Automated integration tools can make the development process more efficient and controlled, but the systems and security specialists must invest the time to learn how these tools work.

Strategy 2: Partial Integration

In the partial integration approach, only mission critical applications are selected for integration. Noncritical applications are networked and remain outside the new system. For example, a large insurance company found it necessary to move to a larger and faster system to handle increased transaction volume. An analyst determined that the claims and provider administration systems were critical. The insurance company integrated them into a single claims and provider administration system. The system was then networked to other applications (e.g., actuarial, general ledger, and member eligibility).

This strategy permits the information security specialist to improve controls over the critical applications during integration of the new system. Older systems are often too difficult and expensive to improve. By using a partial integration strategy, the insurance company achieves a level of integration and improved control of critical applications with a reasonable investment.

Strategy 3: Surround Technology

Surround technology integrates all critical systems on an operating platform that provides significant throughput and processing capability. In this approach, the functions of the applications are not significantly changed; updates are made only to improve processing and throughput. In one example, a university research department received a used supercomputer with applications that had run on older minicomputers and an older mainframe system. These applications were moved to a networked supercomputer environment, which allowed fast access to more terminal connections. Project accounting for grants, reporting for government requirements, grant proposal tracking, and department research projects experienced increased efficiencies in processing, throughput, and information access.

A surround technology strategy improves performance and processing; the security control issues do not change. To enhance the security controls, the information security specialist should consider installing a front-end access control software package.

Strategy 4: Client/Server Processing

Creating a client/server integration strategy is an increasingly popular approach. The increased power of network management systems, routers, relational data bases, and query language has given the end user effective tools to develop client/server applications. For major integration projects, the developer has the option of designing and moving information data bases closer to the client. The developer can convert an application to run locally on a workstation and integrate the necessary communications and editing to the main data base repository.

For example, a large California-based agricultural company relies on a network of sales representatives and customers to market and purchase its products. The company ran a batch-oriented purchase order system and separate inventory control system. The general ledger ran on another separate machine. These systems did not provide distributed online access. As a result, it might take several hours after a sales representative called in an order to receive confirmation that the order could be filled.
A technology steering group of managers, users, and systems staff decided to create a client data base for the sales representatives which included purchase order and inventory update information, and another client data base for the inventory storage facilities. These client data bases were linked to a file server running on a minicomputer. The minicomputer-based data base was updated periodically, and once a day information was downloaded to the general ledger.

A client/server strategy creates a significant challenge for the information security specialist. For example, the security specialist must determine how the client/server configuration will be structured and where information will be stored. The security specialist must thoroughly understand the client/server architecture in order to determine the relative security exposure of each of the client and file server data bases. Controls are selected on the basis of this risk assessment.

Strategy 5: Back-End Processing

Integration through a back-end processor (e.g., an integrated data base) can provide users with a comprehensive reporting facility. The operations and control issues regarding data input, processing, and transfer remain the same. In one case, a regional bank purchased two community banks that had different information processing systems. Converting the new systems was too expensive and time consuming; therefore, the IS conversion team decided to plug these two systems into a large back-end data base processor. Operating information was routed to this processor. Management reports were developed using the query languages available with the data base. Reports of activity at the two community banks could then be compared and reconciled.

In this example, the information security specialist may be able to improve the controls used to consolidate reporting, but he or she is generally unable to change controls for other major systems. There is no opportunity to improve existing applications with ineffective controls.

Recommended Course of Action

The information security specialist can play an important role in the implementation of major systems integration projects. To ensure success, the information security specialist must have a clear understanding of the integration strategy. If such new technologies as client/server processing are used, the security specialist must take the time to learn about this technology. It is also important that the security practitioner understand the critical business reasons for the integration project.

The security specialist should consider how to advise the systems integration team. One recommended course of action includes these activities:

- Develop an information security integration work plan based on the type of integration project being implemented.
- Address the three factors—human, technical, and financial—involved in the failure of systems integration projects.
- Create an information security program focused on general controls, application controls, network controls, operating systems controls, recovery controls, and access controls.
- Determine the level of risk for the areas mentioned in the previous step and identify the controls that merit implementation and enhancement. Exhibit 2 rates the risks for each of the five integration strategies.
· Allocate information security resources on the basis of risk within a reasonable budgetary level.

· Work with managers, developers, business users, and auditors to ensure adequate information security coverage.

## Ratings of Information Security Risks

<table>
<thead>
<tr>
<th>INFORMATION SECURITY FOCUS</th>
<th>INTEGRATION</th>
<th>Partial Integration</th>
<th>Surround Technology</th>
<th>Client/Server</th>
<th>Back-End Processing</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Controls</td>
<td>High</td>
<td>Medium</td>
<td>Medium</td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td>Application Controls</td>
<td>High</td>
<td>High</td>
<td>Medium</td>
<td>Medium</td>
<td>Low</td>
</tr>
<tr>
<td>System Controls</td>
<td>High</td>
<td>High</td>
<td>High</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Communication Controls</td>
<td>Medium</td>
<td>High</td>
<td>High</td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td>Backup and Recovery Controls</td>
<td>Medium</td>
<td>Medium</td>
<td>Medium</td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td>Access Controls</td>
<td>High</td>
<td>High</td>
<td>Medium</td>
<td>High</td>
<td>Low</td>
</tr>
</tbody>
</table>

Integration projects represent an opportunity for the security specialist to implement and strengthen controls in a cost-effective way. The approach described in this article can serve as a model for improving controls given specific integration strategies and business environments.

### Author Biographies

Steve Mar  
Steve Mar, CISA, is a manager with KPMG Peat Marwick in San Francisco. He specializes in information systems audits, security, and business resumption.