Deloitte & Touche

IT Architecture Review

ISACA Conference Fall 2003

Table of Contents

Introduction

IT Architectural Design:

The advent of the internet has created powerful new business processes as well as emerging risks for IT Risk management.

The objective of this track is to ensure that IS auditors can effectively evaluate an organization's architecture and technical infrastructure.

The content covers the development, acquisition and implementation of IS architectures and associated operational practices to ensure efficiency and information security.

Business Drivers

- Potential drivers for the implementation of N Tier Architecture
  - Limitations of the Classic Architecture
    - Low Flexibility
      - Difficult to enhance systems functionality or expand into new products
    - Poor Scalability
      - Scalability is costly and limited by the architecture's design
  - Competitive Factors
    - Barriers to Entry
      - Ease of competitor's entering the market
  - Strategy
    - Globalization
      - Ability to implement regionalized ecommerce sites

Overview of Tiered Architecture

Client-Server Paradigm (1 of 3)

- Client/server architecture
  - Introduced in the early 80's
  - clients and servers are separate logical objects that communicate with each other to perform a task together
- No physical connection between a client and a server
  - Reside on the same machine
  - Reside on two separate machines across a network
  - Applications can be deployed on different hardware and different operating systems, optimizing the type of work each performs

Client-Server Paradigm (2 of 3)

- Clients
  - Entities that request services of another computer system or process using an established protocol and accept the server's response
  - Client makes a request for a service and receives a reply to that request

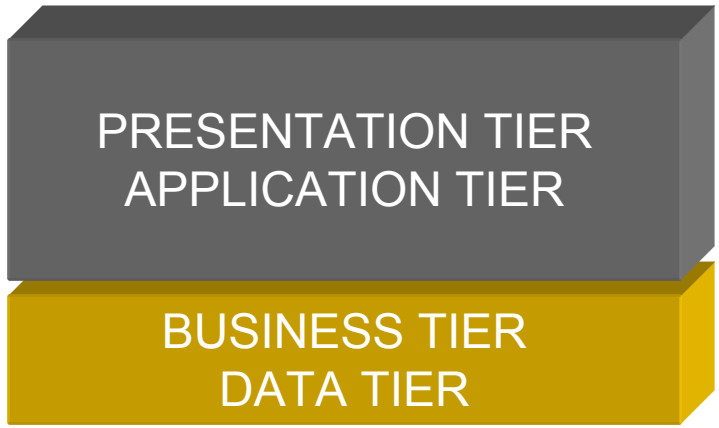
- Servers
  - Entities that provide requested services
  - Server waits, receives, processes requests and then sends back a response

Client-Server Paradigm (3 of 3)

- Benefits of client/server architectures
  - Code is re-usable
    - When properly designed, the same code may be used in many different instances
    - One may design a system that responds automatically to increase in system load by adding new servers and services without too much difficulty
  - Modular and Extensible
    - Allows for fault tolerant systems
    - One service can be offered on many different machines
    - No single point of failure

Tiered Architecture (1 of 2)

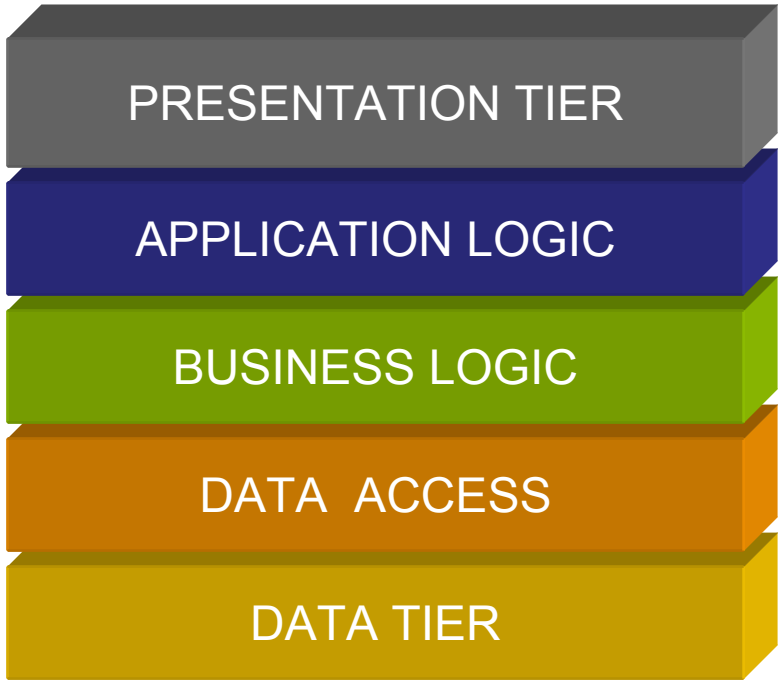
- Classic two-tier "Fat-Client" model:
  - Tier One: Customer access system and gateway services. Also performs presentation and customer application services
  - Tier Two: Provides business logic and database services



- Disadvantages:
  - Poor Scalability
  - Maintenance – upgrades have to be deployed to all clients

Tiered Architecture (2 of 2)

- N Tier Architecture
  - Tier One: Client side: browser/WAP/PDA. Server side: Markup tags
  - Tier Two: Data Encryption, Port Assignments
  - Tier Three: Business objects and Rules, Data Transformation
  - Tier Four: Data Access Objects, ODBC, JDBC, XML
  - Tier Five: Data Repositories
- Abstraction
  - Layers are Independent
- Advantages
  - Reduces maintenance costs and increases functional flexibility in the long run



IT Architecture Review

IT ARCHITECTURE REVIEWS

- Why review IT architecture
- How to conduct IT architecture reviews
- What to review and assess
- Performing the assessment

Why Review IT Architecture

- IT architecture is a key component in supporting business goals and objectives:
  - Foundation for developing large, complex, distributed systems environment;
  - Manage and control complexity in system deployment;
  - Basis for determining software and hardware decisions
- Defines the overall IT goals, organization and system components needed to support long-term business requirements
- Identify gaps and areas for concern or improvement
- Optimize return on IT /IS investment

How to Conduct IT Architecture Reviews

- Define business goals and objectives
  - Identify existing IT and systems infrastructure environment:
    - the structure and organization of IT /IS in supporting business goals
    - the architectural framework (layers) for developing and connecting system components
  - Review and Identify gaps between architecture characteristics / attributes and business requirements

What to review and assess

- Logical - functional requirements of IT architecture
  - Abstraction & encapsulation
  - Information hiding
  - Separation
  - modularization
- Process – abilities of the system that can be measured
  - Flexibility
  - Security
  - Scalability
  - Performance
  - Reliability
  - Availability
  - Maintainability
- Infrastructure – Physical infrastructure and system components

Non-Functional Requirements (1 Of 2)

- Scalability
  - May be expanded or reduced in size to meet business requirements
  - Bottlenecks can be resolved by adding more hardware/memory/processing power
  - constraints are not imposed by the software
  - ability to easily adjust for the number of concurrent users, data storage requirements, network capacity, and so forth
- Reliability
  - Systems perform consistently in both normal and adverse conditions within the accepted operational cycle (24x7) and system downtime
  - In the event of hazards, peak traffic loads, or attacks, systems appear to operate smoothly to users while allowing for intuitive, effective management and recovery by the staff
  - Eliminates single points of failure
- Flexibility
  - The ability to expediently add new products and services to the architecture in response to business needs
  - Essential to providing flexibility is designing code as discrete, re-useable modules in addition to selecting products that support well-known standards
  - Avoiding product customization when integrating the components to the architecture also aids flexibility

Non-Functional Requirements (2 Of 2)

- Performance
  - Good performance means the interval from the time the user enters a request to the time a response is received encourages use of the system
  - Performance factors include the ability to quickly route HTTP traffic, handle SSL sessions, complete a transaction, and return a third-party service

- Manageability
  1. *Operational* - All non trivial systems contain the instrumentation to be proactively managed by an administration tool. Responses to messages from nodes (e.g. SNMP traps) are automated and sophisticated. Management traffic is not excessive and a burden to the network
  2. *Development Approach* – The design of the architecture facilitates code re-use and efficient debugging. The manner in which services and logic are partitioned within the architecture is intuitive and results in components playing discrete, well-defined roles

Infrastructure Requirements

- Ability to Duplicate
  - It is possible to replicate the system at another location
  - The architecture is transparent at the conceptual level, and its components are suitable for an international environment (e.g. well-known abroad, available in foreign languages)
- Acceptable Cost of Operation
  - Considering alternative approaches and comparable business requirements, the total cost of ownership of the resulting environment is within the lower quartile
- Long-Term Viability
  - The design of the architecture is based on state-of-the-art yet proven concepts and built using best of breed products.

Infrastructure Components

- Logical view of the architecture helps one understand how the infrastructure fits together at a conceptual level
- Ultimately products must be selected to support the high-level design
- These products become the actual "components" or "building blocks" of the architecture that are installed and configured to support operations

Infrastructure Components

1. **Clients**
   - e.g. web browsers or telephones connecting to the IVR (Interactive Voice Response), using company resources and services

2. **Network components**
   - Includes firewalls and web traffic dispatchers

3. **Web servers**
   - Handles HTTP requests and securing communications via SSL

4. **Application servers**
   - Focuses on presentation and session management services

Infrastructure Components

5. **Business logic and transaction servers**
   - Manage and execute transactions

6. **Database servers**
   - Data storage and management

7. **Server Operating Systems**

8. **Development languages and tools**
   - Create logic, design GUI interfaces, and customize services

9. **Network and systems management tools**
   - Monitor and manage system / network events

Performing the Assessment - Example

Example: Performing the Assessment

- Areas to consider for assessment: Information Resource Planning, Business Continuity Planning, Architecture Development, and Security

Assessing IT architecture security –

- Consider the risks and implemented strategies to mitigate potential security hazards. Any general security strategy should be include controls to:
  - prevent;
  - detect;
  - control; and
  - respond to architectural security.

  – Review the organizational Internet security strategy
  – Identify and assess controls contributing to each of the above.

Performing the Assessment

- *What to ask:*
  - Has the organization established Internet security policies and procedures as part of its general information protection strategy?
  - What types of authentication technology are in use within the network (i.e. single sign-on, token technology, call & response, certificate authorities)? How are these technologies integrated with the Internet technologies?
  - Is adequate security implemented throughout the network (i.e. from client to web server, from web server to backend system, from web server to database, etc)?
  - Does the organization use encryption technology to protect transmitted data (internal and/or external transmissions)?

Performing the Assessment

- *What to ask:*
  - Does the organization have its public Internet servers certified by a certificate authority, such as Verisign to protect against imitation servers on the public network.
  - Does the organization employ any types of virus protection technology to mitigate the risk of introduction of destructive items from the public network?
  - What types of security tools/utilities are in use?
  - Where are Internet servers deployed, inside or outside the firewall?
  - How are security breaches detected and communicated?
  - What procedures are followed to neutralize security threats once they are detected?
  - Do audit procedures exist to periodically review the security status of the network and Internet systems and identify instances of potential threatening activity?
  - Are audit logs being recorded (audit tools and/or the operating system) and reviewed regularly?

Performing the Assessment

What to do:

- With the assistance of technical personnel, audit staff, and IT audit management, identify significant risk issues associated with Internet control, security, and audit.
- Review existing security policies and procedures and confirm adequacy given organizational standards.
- Review security configurations of operating systems, Internet applications, and other utilities/tools (if applicable). Confirm that settings meet organizational standards.
- Consider the use of computer assisted audit tools to interrogate status of significant hardware components and report potential security risks.

Performing the Assessment

What to do:

- Test and confirm that security controls are implemented over each significant entity within the network (i.e. firewall, web server, applications, database, etc).
- Test and confirm the functionality of encryption utilities.
- Test and confirm the functionality of implemented virus protection tools by reviewing tool configurations and reviewing incident logs.
- Test and confirm the adequacy of audit log settings.
- Test and confirm the adequacy of incident response procedures.

Relevant Issues

Relevant Issues

- Information Security
- Software Development Lifecycle

Information Security (1 of 3)

- Issue: Privacy of Customer Data
  - Personally Identifiable Information vs. Non-personal Information

- Relevant Concerns
  - Loss of Customer Trust
  - Loss of Brand Value
    - SB1386 requires that a company "…disclose in specified ways, any breach of the security of the data, as defined, to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person"

Information Security (2 of 3)

- Examples Include:
  - JetBlue Airways
    - Violated its own privacy policy
    - Provided 5 million passenger itineraries to a Defense Department contractor that used the information as part of a study seeking ways to identify "high risk" airline customers”
  - FTC Study
    - 1 in 7 Americans are victims of Identity Theft

Information Security (3 of 3)

- Examples of Control Weaknesses
  - Use of live customer data in a Test environment
  - Inappropriate User Access to Customer data
  - Data Encryption does not exists at all levels

Systems Development Life Cycle (1 of 2)

- Issue: Segregation of Environments, Coding Standards

- Relevant Concerns
  - Inappropriate access
  - Application Instability
  - Maintenance Issues

Systems Development Life Cycle (2 of 2)

- Examples of Control Weaknesses
  - Developer with access to both test and production environments
  - Poor abstraction between presentation, logic and data
    - e.g. HTML tags or business logic in the data layer

Q & A

- Questions