



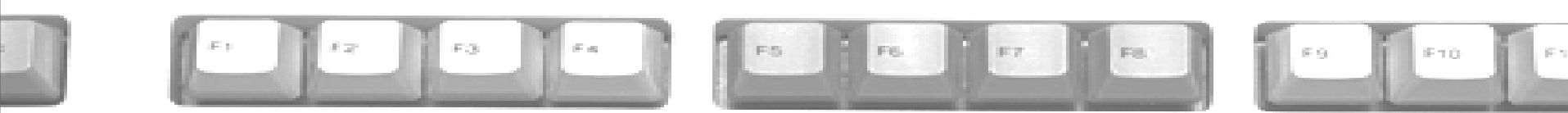
ISACA Fall eXciting Seminar 2003

***Introduction to Project Risk
Management and SDLC Reviews***

Greg Thomas

Deloitte & Touche LLP

October 2004



Objectives

Upon completion of this presentation, participants will:

- Understand the principals of Project Risk Management and Systems Development Life Cycle reviews
- Be able to identify the key risk areas associated with projects



Key Concepts

IT Risk Management

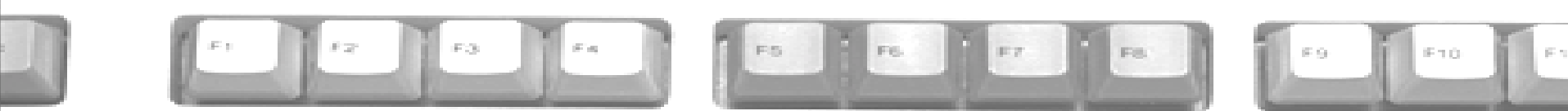
The policies, procedures and processes used to mitigate risk in the IT environment.

Project Risk Management (PRM)

Project Risk Management is a function of *IT Risk Management*. PRM policies, procedures and processes help ensure projects are delivered on schedule within budget and meet business objectives.

Systems Development Life Cycle (SDLC)

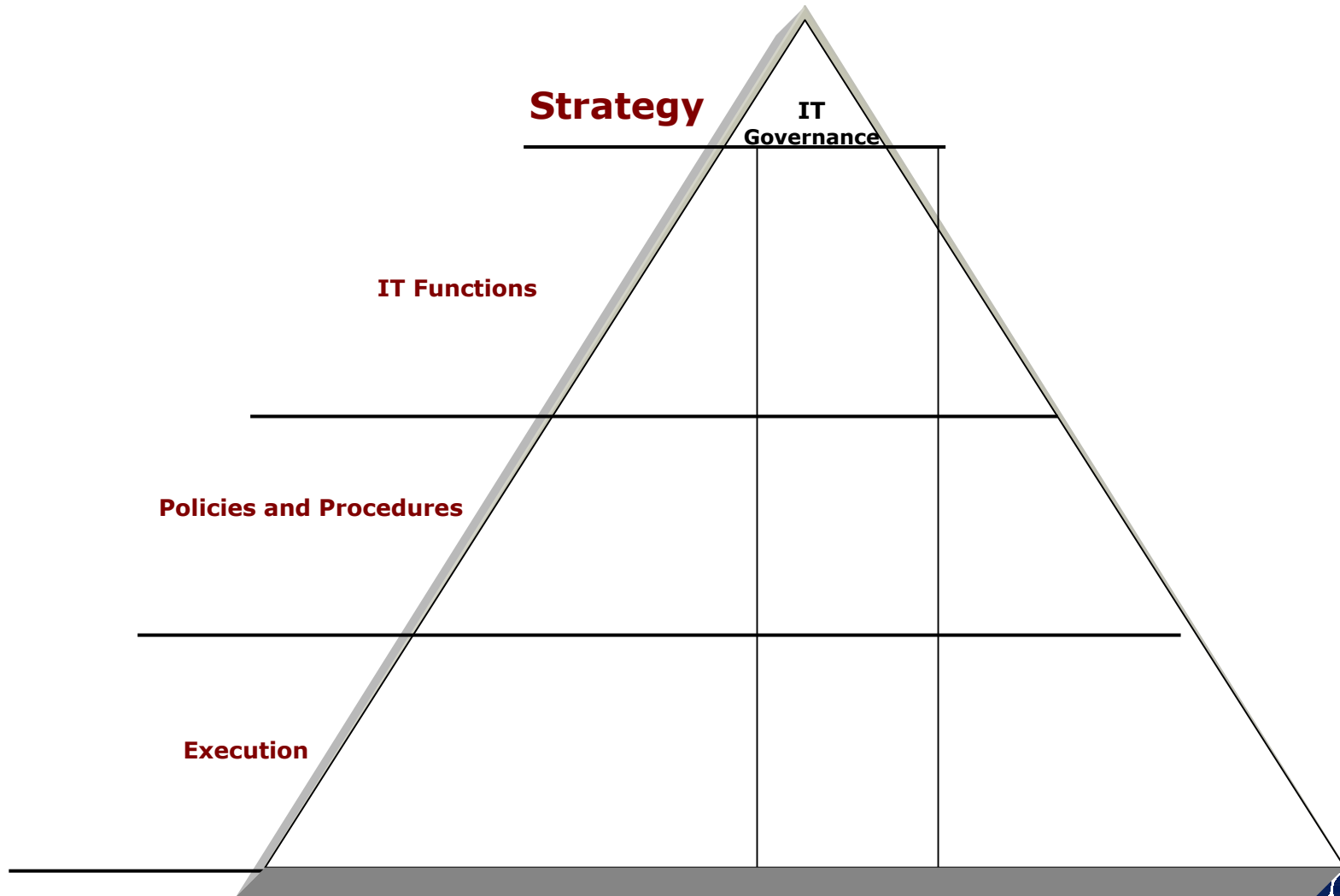
The *Systems Development Life Cycle* is a set of PRM policies and procedures that help guide a project from concept to implementation.



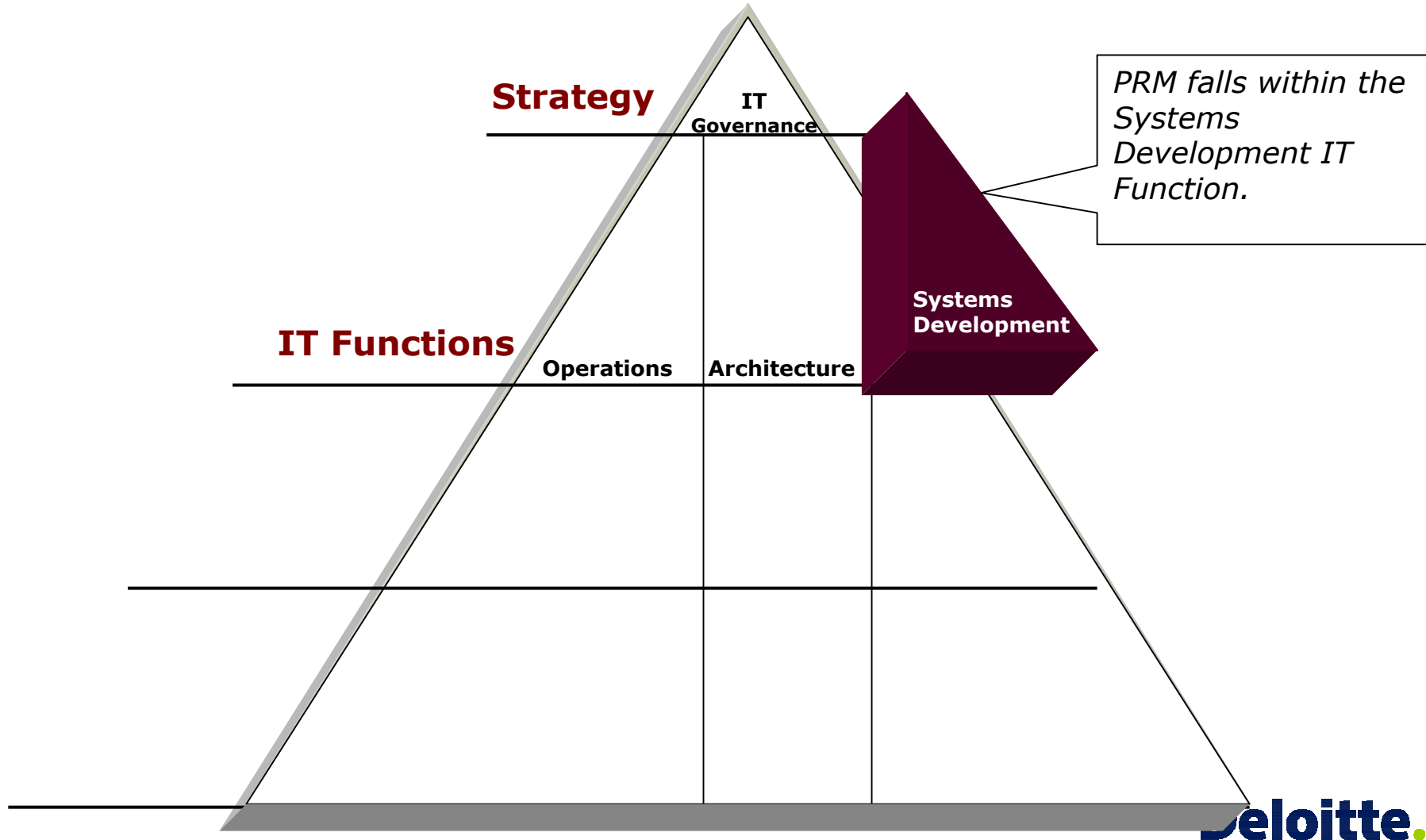
Defining IT Risk Management and Project Risk Management



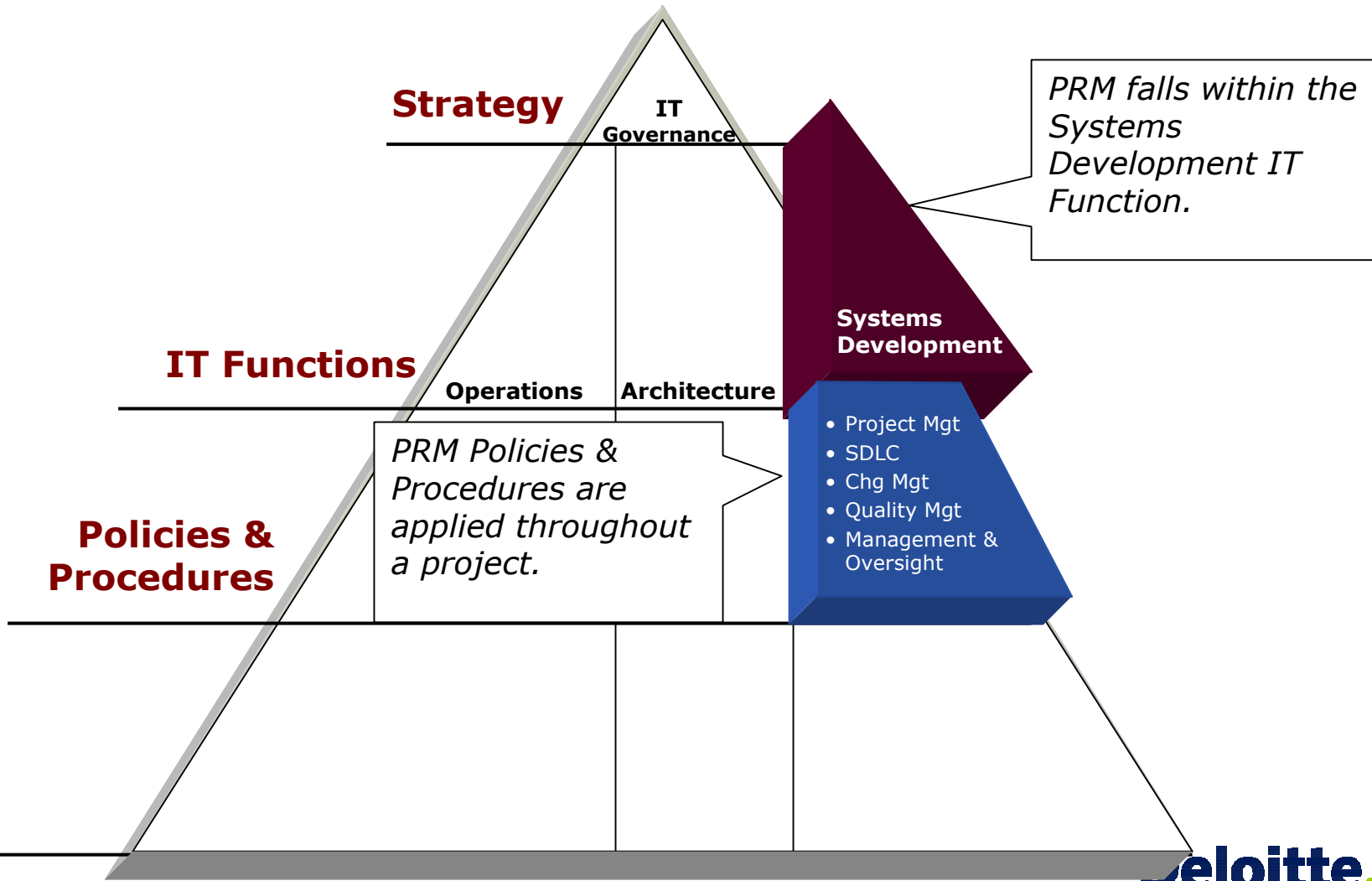
The IT Risk Pyramid



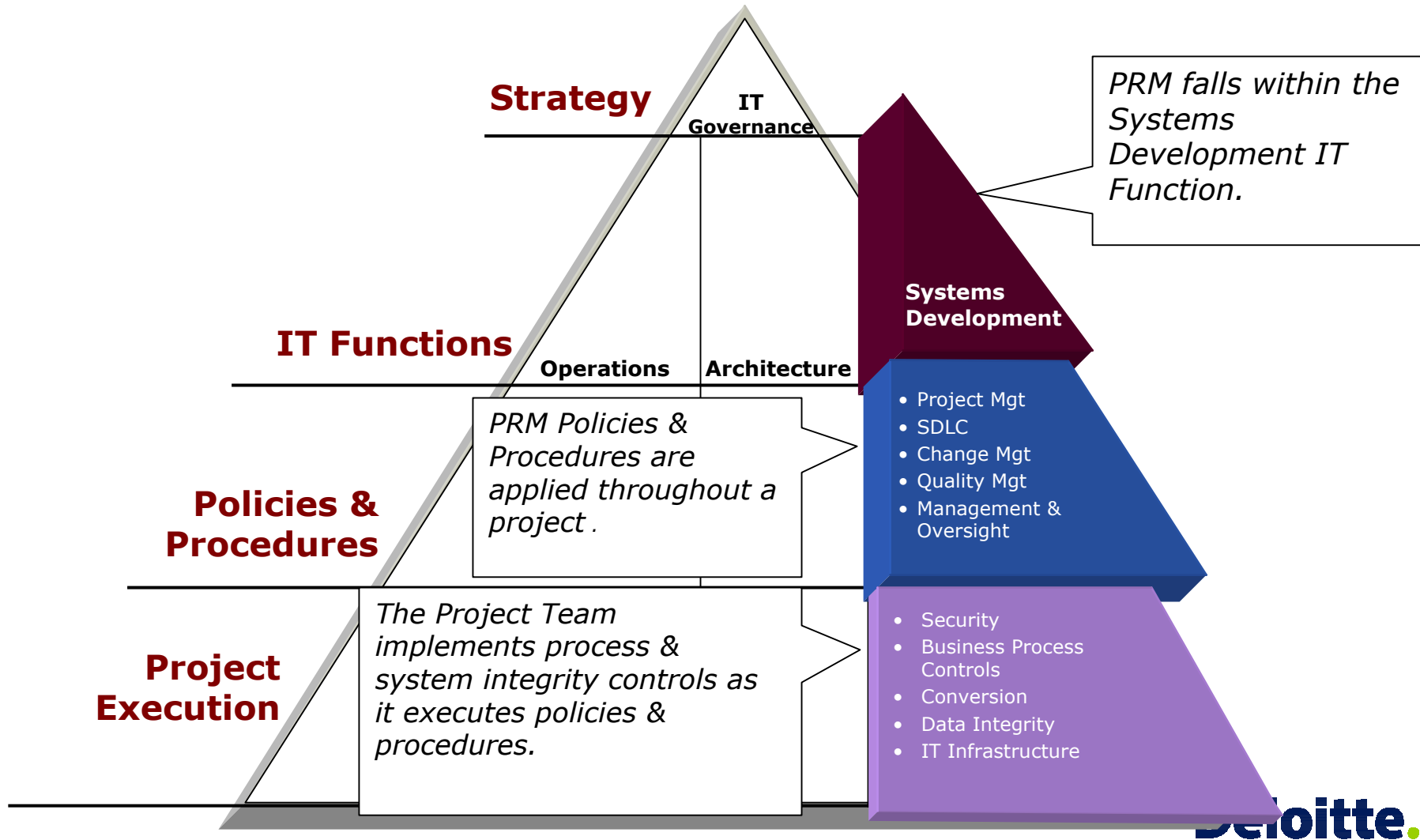
IT Functions, Systems Development & PRM



PRM Policies and Procedures within Systems Development

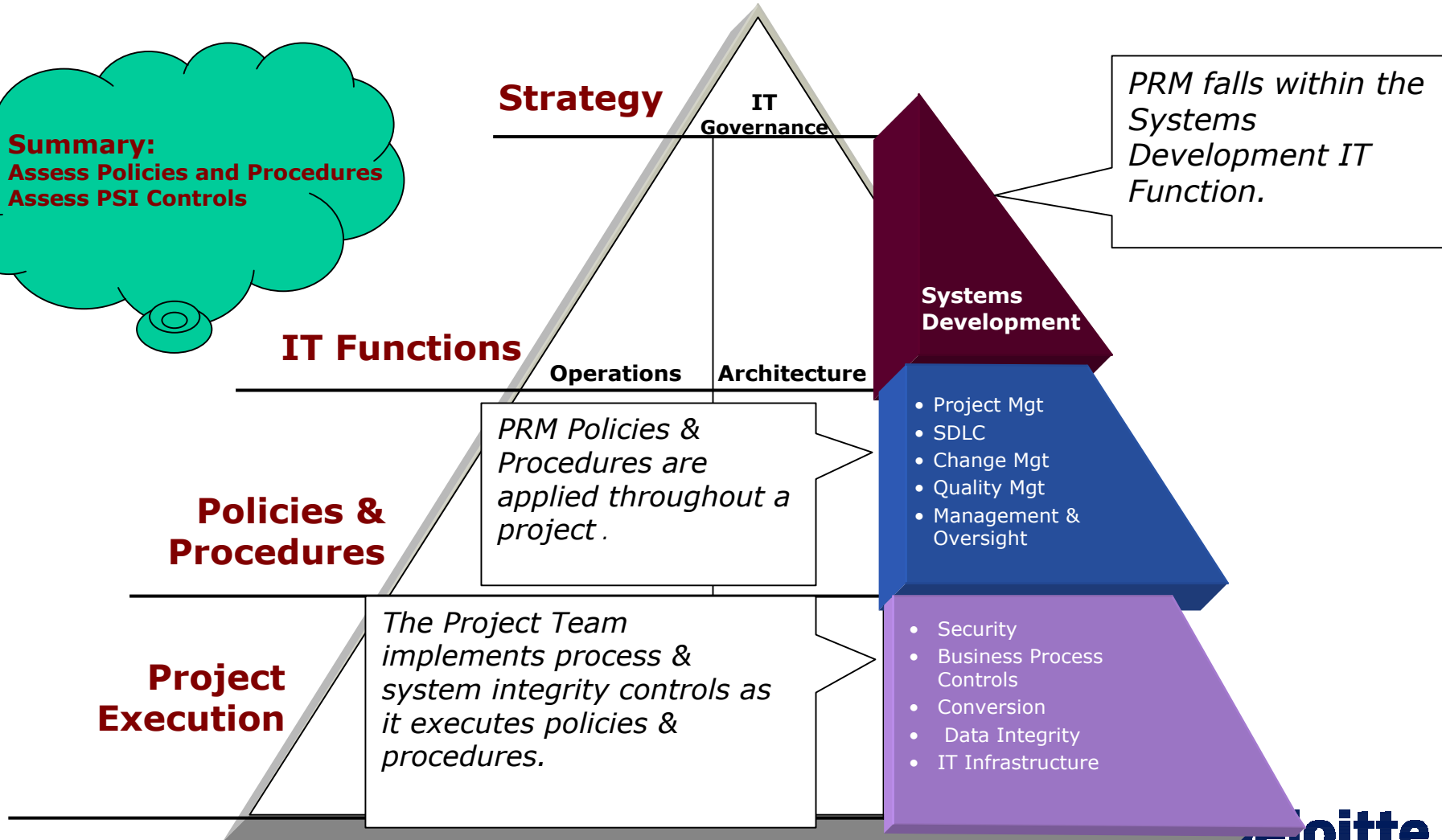


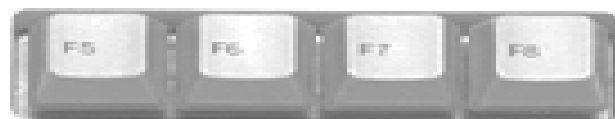
Process & System Integrity within PRM Policies & Procedures



Process & System Integrity within PRM Policies & Procedures

Summary:
Assess Policies and Procedures
Assess PSI Controls





Auditing for Project Risk Management



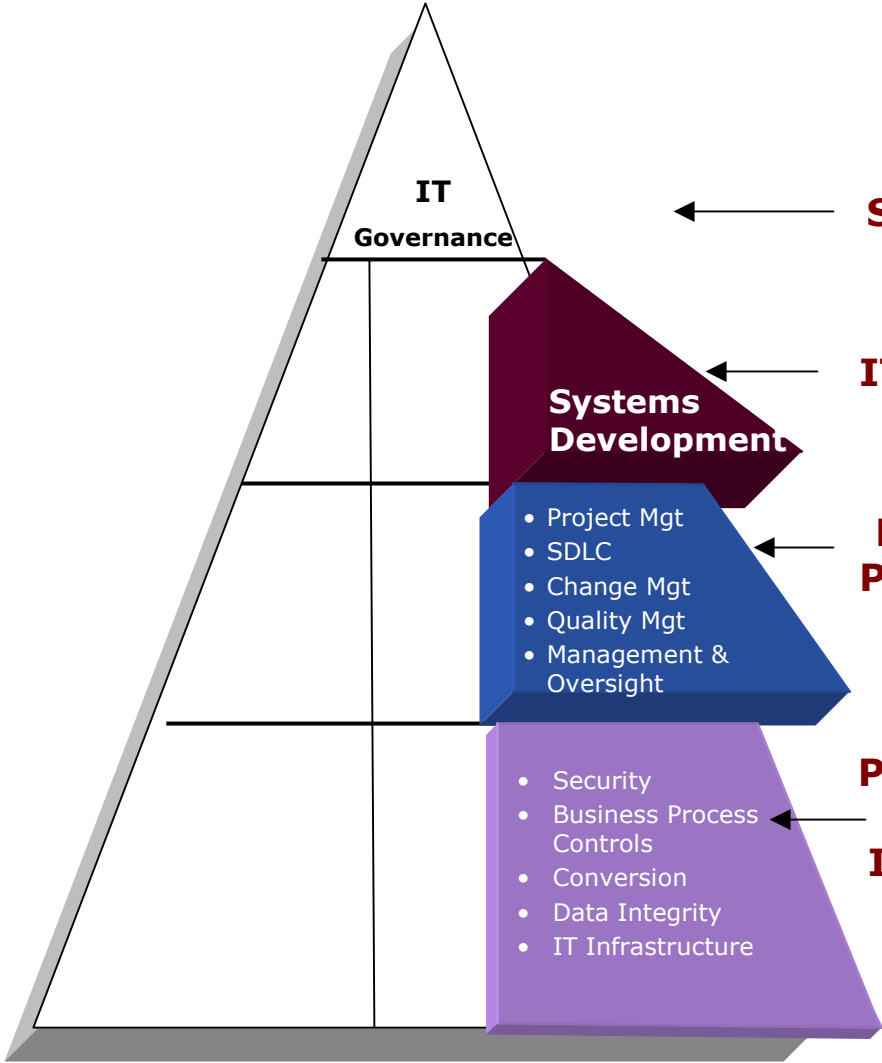
PRM: Policies & Procedures

- 1. Project Management:** The process by which projects are managed.
- 2. Systems Development Life Cycle:** The process through which projects move from concept to implementation.
- 3. IT Change Management:** The process by which change in the IT organization is managed.
- 4. Quality Management:** Independent oversight built into the SDLC to ensure PRM is occurring.
- 5. Management & Oversight:** The organizational structure & controls supporting PRM.

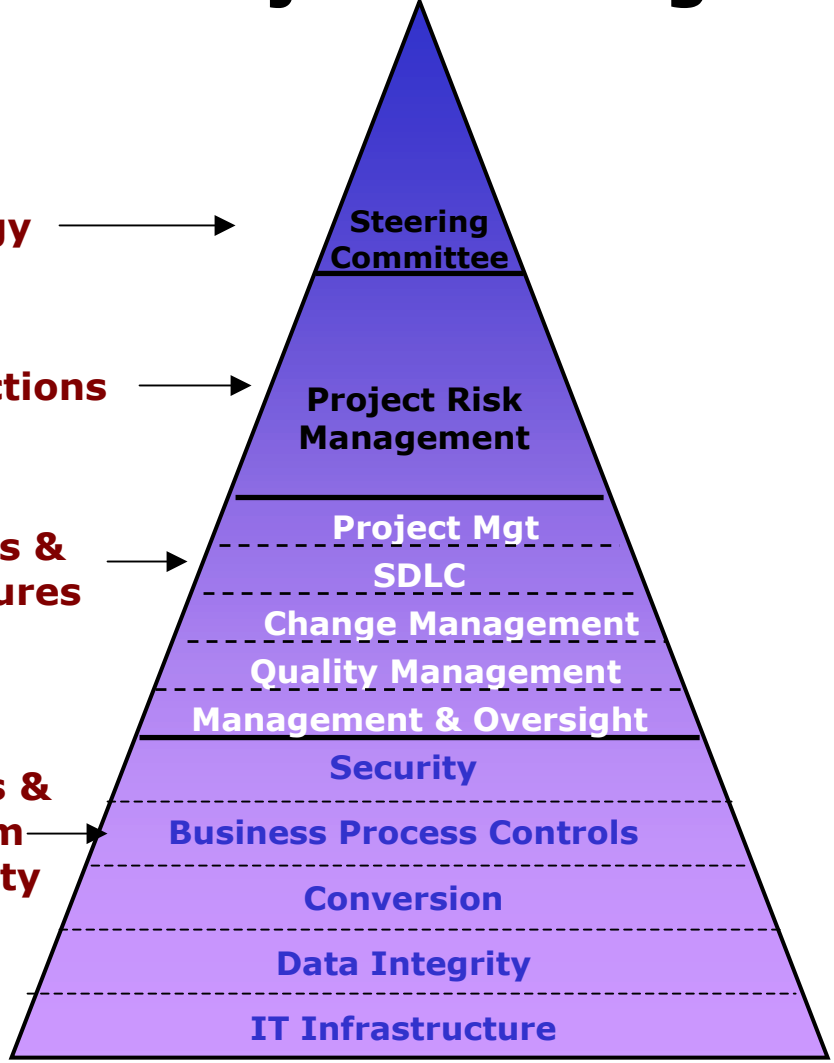


Auditing for PRM Policies & Procedures

IT Risk Mgt



Project Risk Mgt



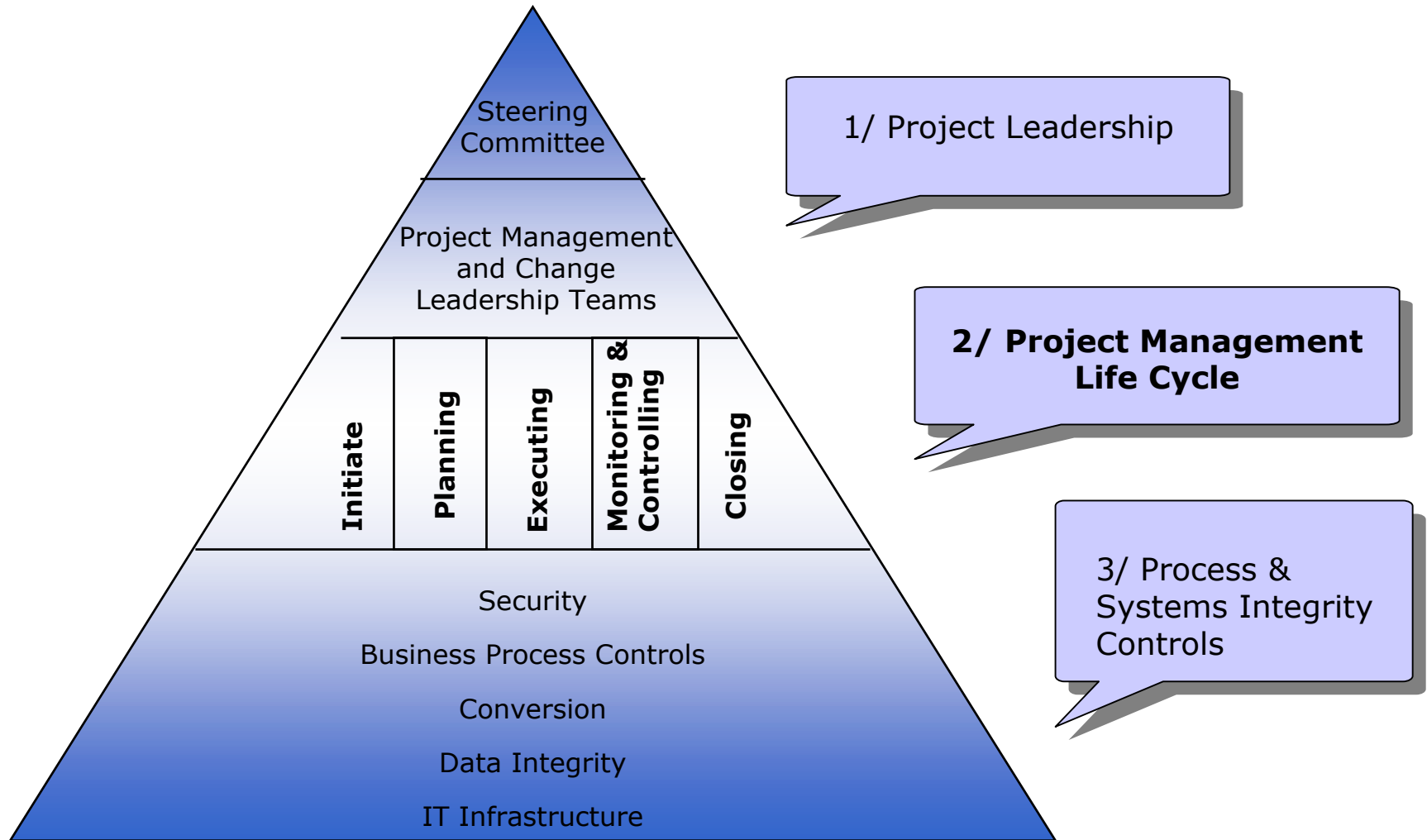
← **Strategy** →

← **IT Functions** →

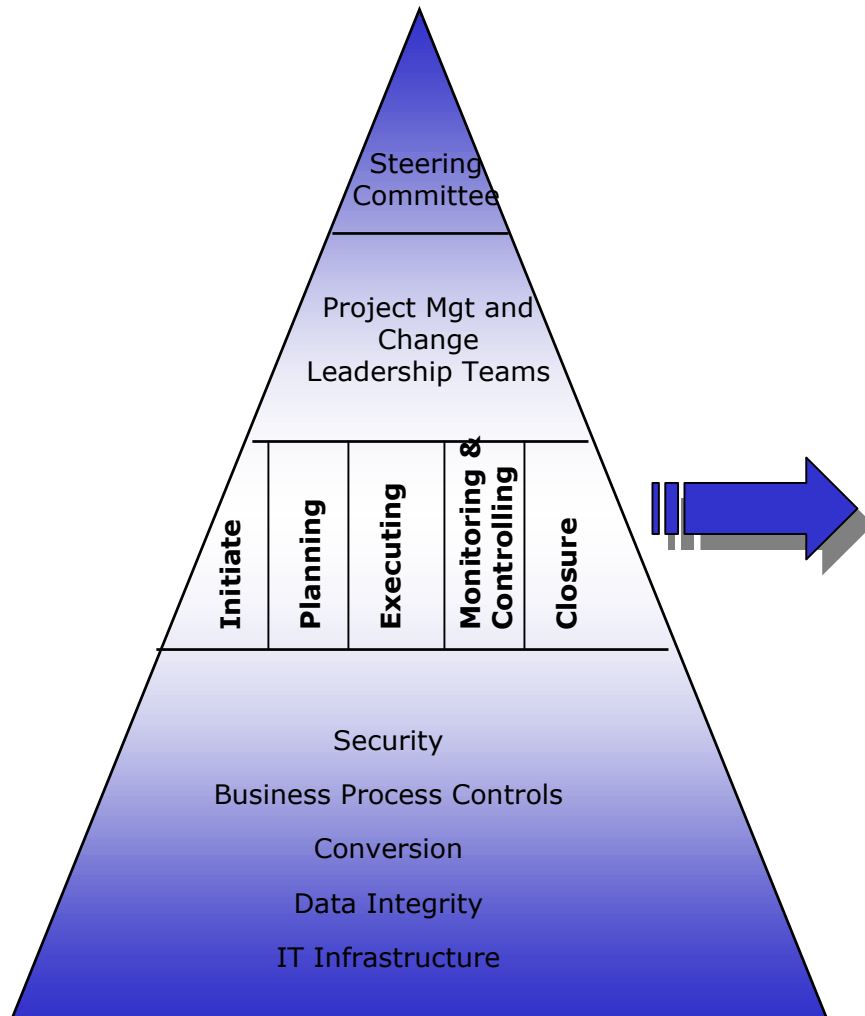
← **Policies & Procedures** →

← **Process & System Integrity** →

Project Management Life Cycle



Project Management Controls



Initiate Phase: Project recognition, scope definition and project team organization.

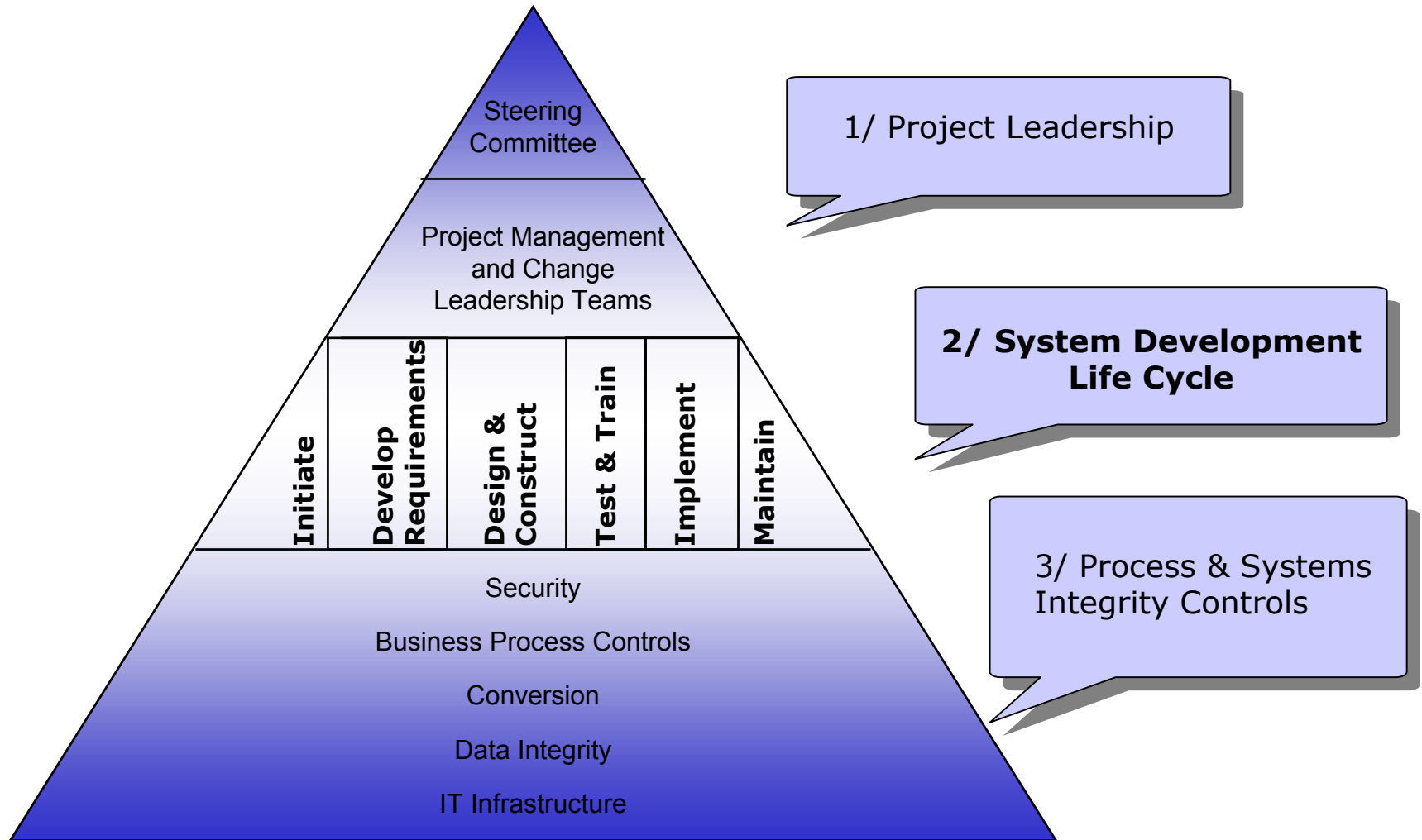
Planning Phase: Create a high level work plan, confirm scope, identify resources, establish a budget, establish reporting structure and define escalation procedures.

Executing Phase: Execute the plan, coordinate communication, ensure consistent use of methodology, initiate reporting procedures.

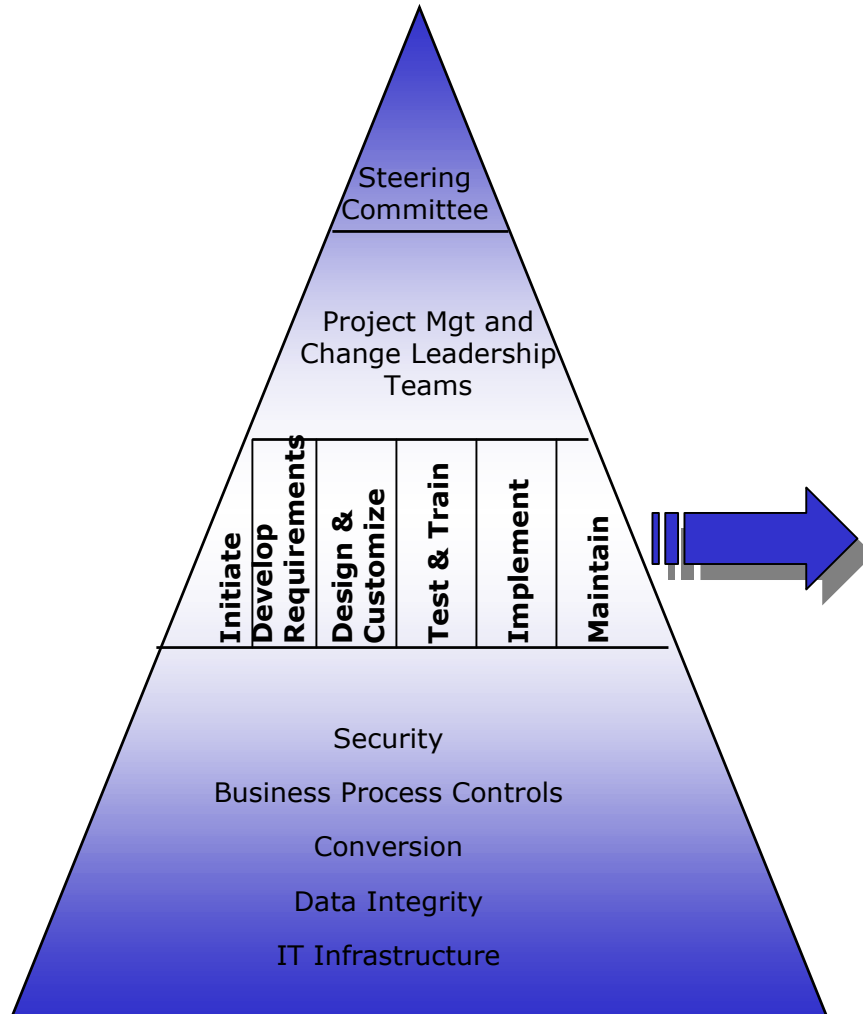
Monitoring & Controlling Phase: Monitor and measure progress regularly, implement project change control procedures, control scope creep, ensure training plans exist, identify and resolve problems.

Closure Phase: Formalize acceptance of the project, conduct post-project reviews.

System Development Life Cycle



System Development Life Cycle Controls



Initiate Phase: Controls are defined to align project interpretation to business imperative.

Develop Requirements Phase: Controls are defined to ensure project requirements meet business needs.

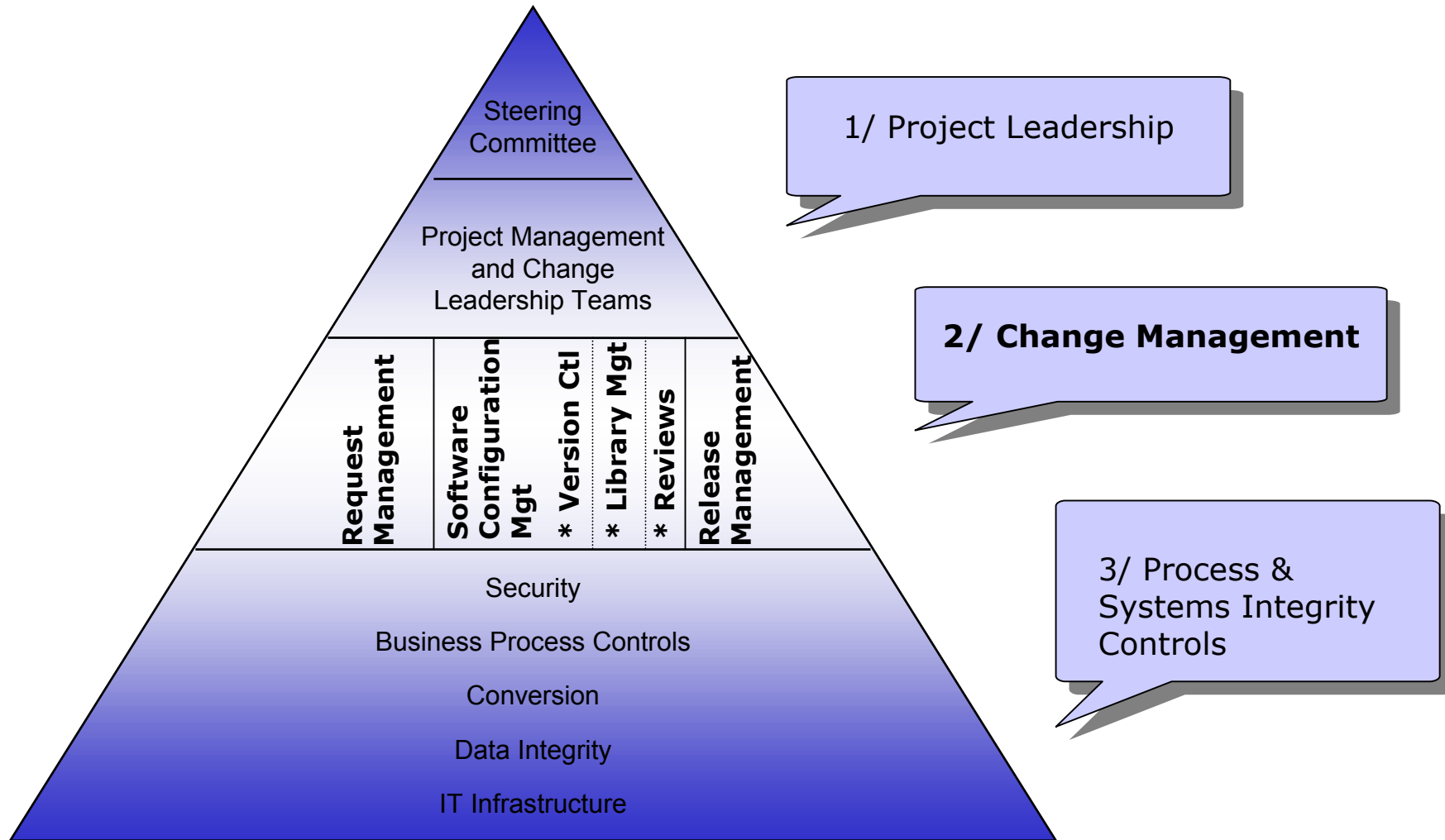
Design & Customize Phase: Controls are defined to ensure design meets requirements.

Test & Train Phase: Controls are defined to ensure all developed objects meet requirements and design. Personnel are trained in use of project deliverables.

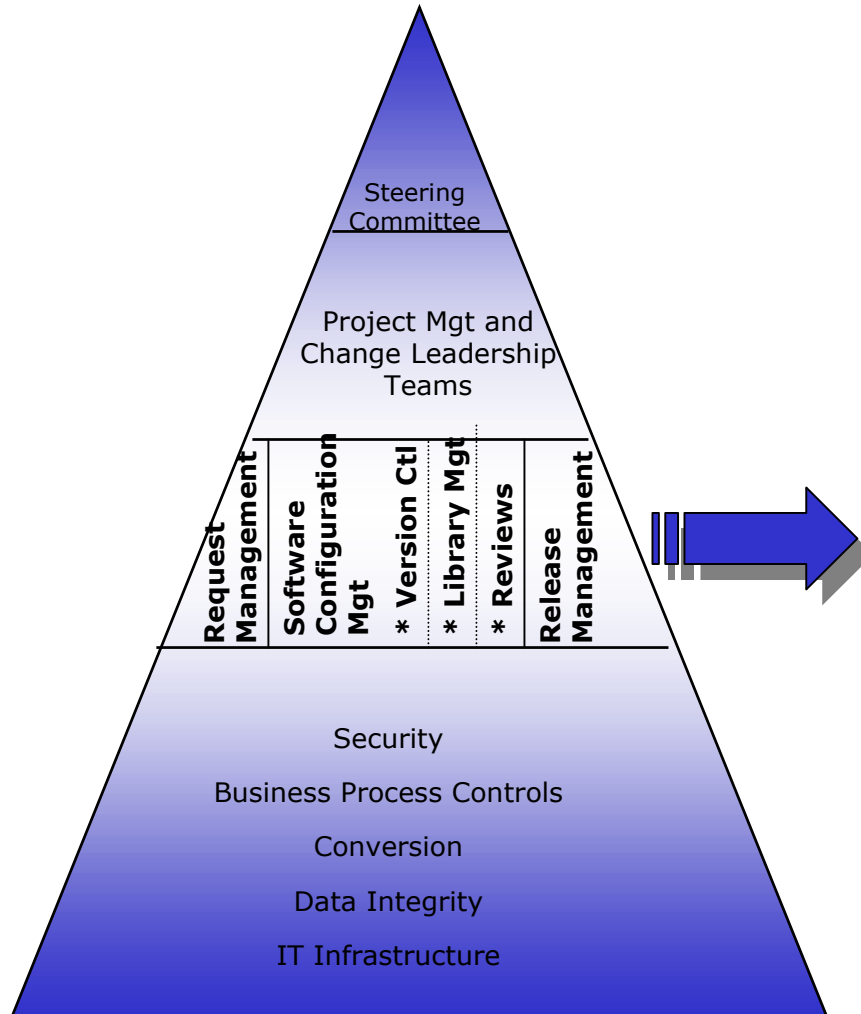
Implement Phase: Controls are defined to ensure smooth and timely implementation of project deliverables.

Maintain Phase: Controls are defined to ensure continued maintenance.

Change Management



Change Management Controls



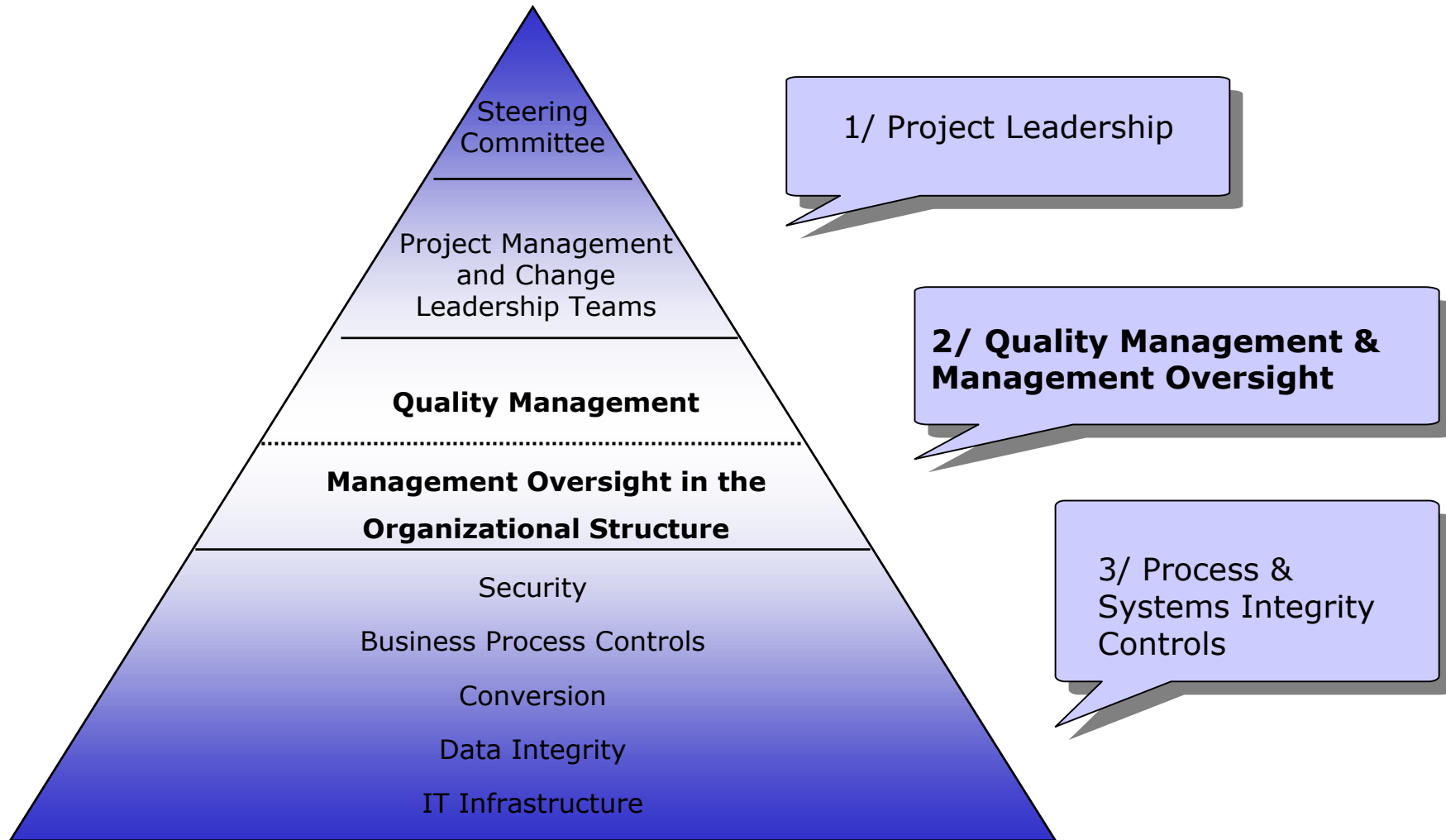
Request Management: The process for identifying, tracking, documenting and approving change requests. Includes impact assessments and feasibility studies.

Software Configuration Management: Technical change management comprised of three components:

- Version Control – controlling multiple releases of changes
- Library Management – object storage and retrieval procedures, parallel development procedures
- Reviews – practices for ensuring adherence to SCM protocols

Release Management: The process for communicating, scheduling and releasing changes into production.

Quality Mgt & Management Oversight





Quality Mgt & Management Oversight



Quality Management: Procedures built into each set of PRM policies and procedures to ensure all quality checkpoints are met during system development. Project Managers are responsible for ensuring that all Quality Management gateways are completed before signing off on deliverables.

Management and Oversight: The organization structures that supports the entire PRM process. Organizational structure may include:

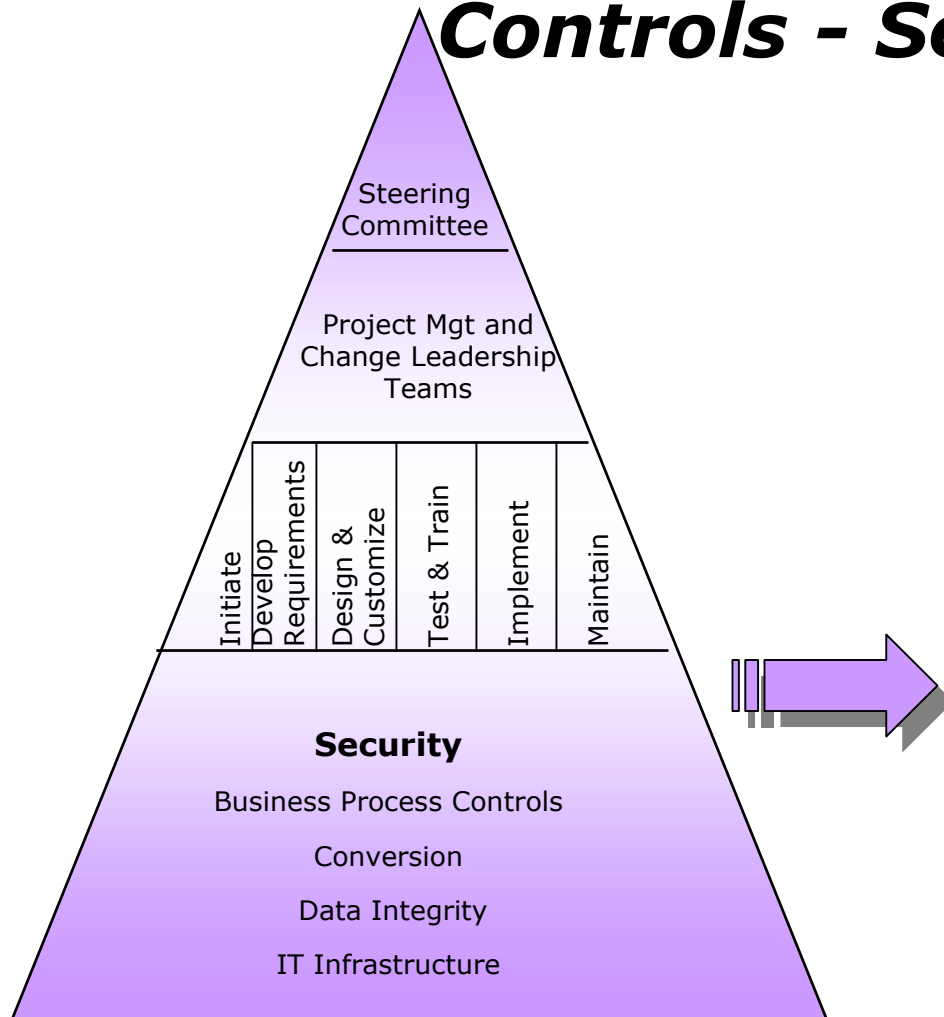
- Software Control Boards
- Production Control Boards
- Change Review Boards
- Change Approval Boards



Auditing for SDLC Process System Integrity Controls



SDLC Process & System Integrity Controls - Security



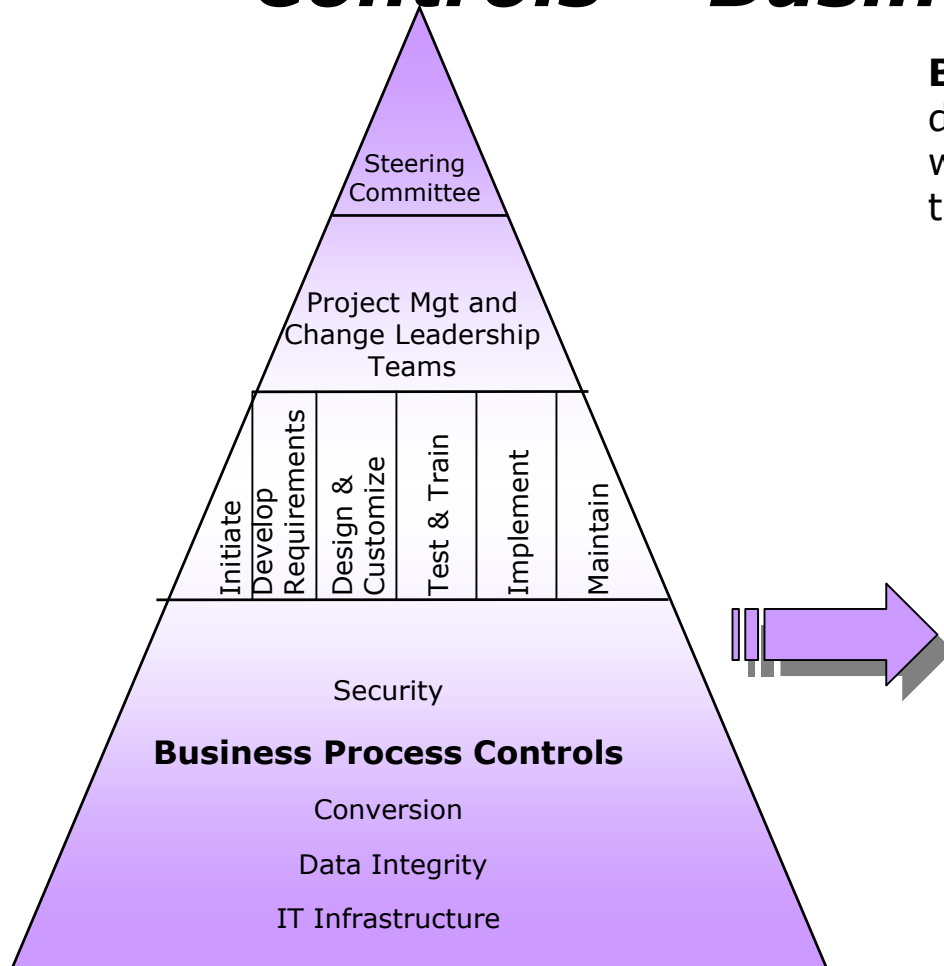
Security controls are built into the design, development, and testing areas of the project. Controls include:

- Application security roles to enforce segregation of duties
- Security over Application Configuration
- Security over the Database used by the Application
- Application security testing

Process and system integrity controls are applied to every phase of the System Development Life Cycle



SDLC Process & System Integrity Controls – Business Process



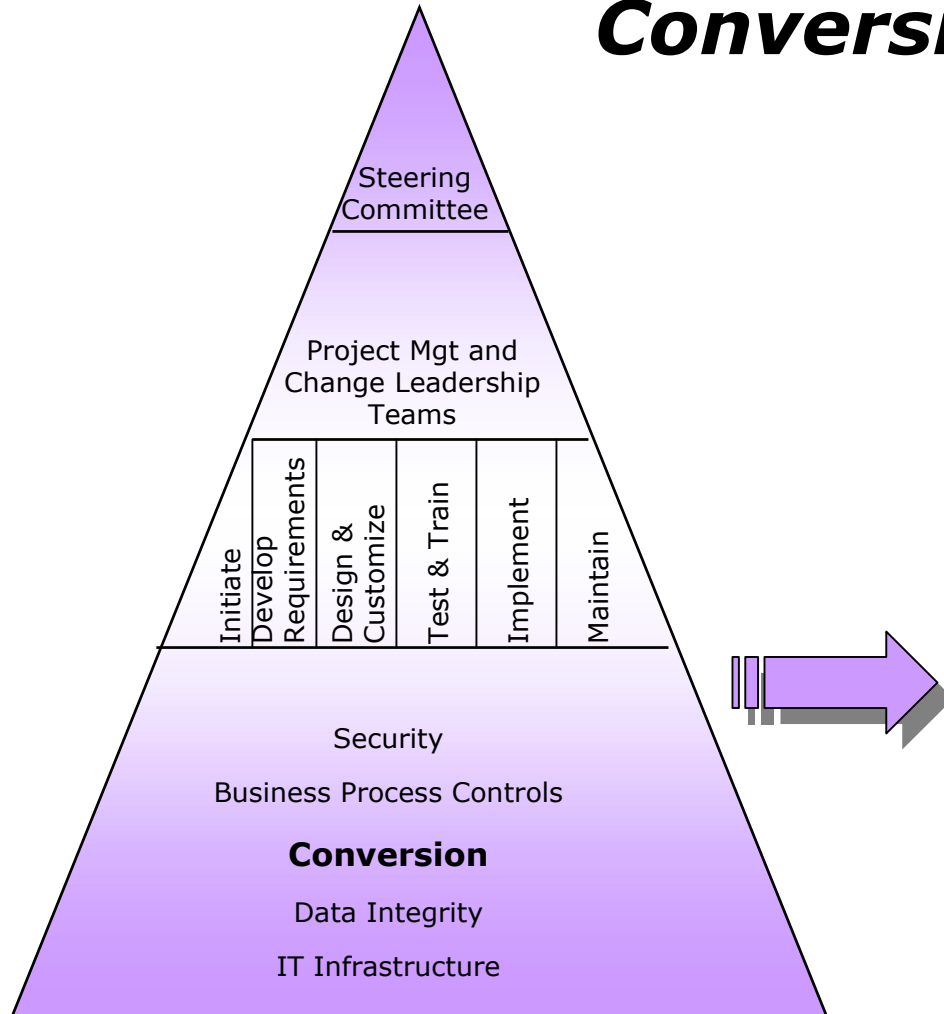
Business Process Controls are designed, developed and tested along with technical requirements throughout the SDLC. Controls include:

- “As-Is” and “To-Be” business processes
 - Manual and Automated
- Design, Development, and Testing Processes

Process and system integrity controls are applied to every phase of the System Development Life Cycle



Process & System Integrity Controls - Conversion



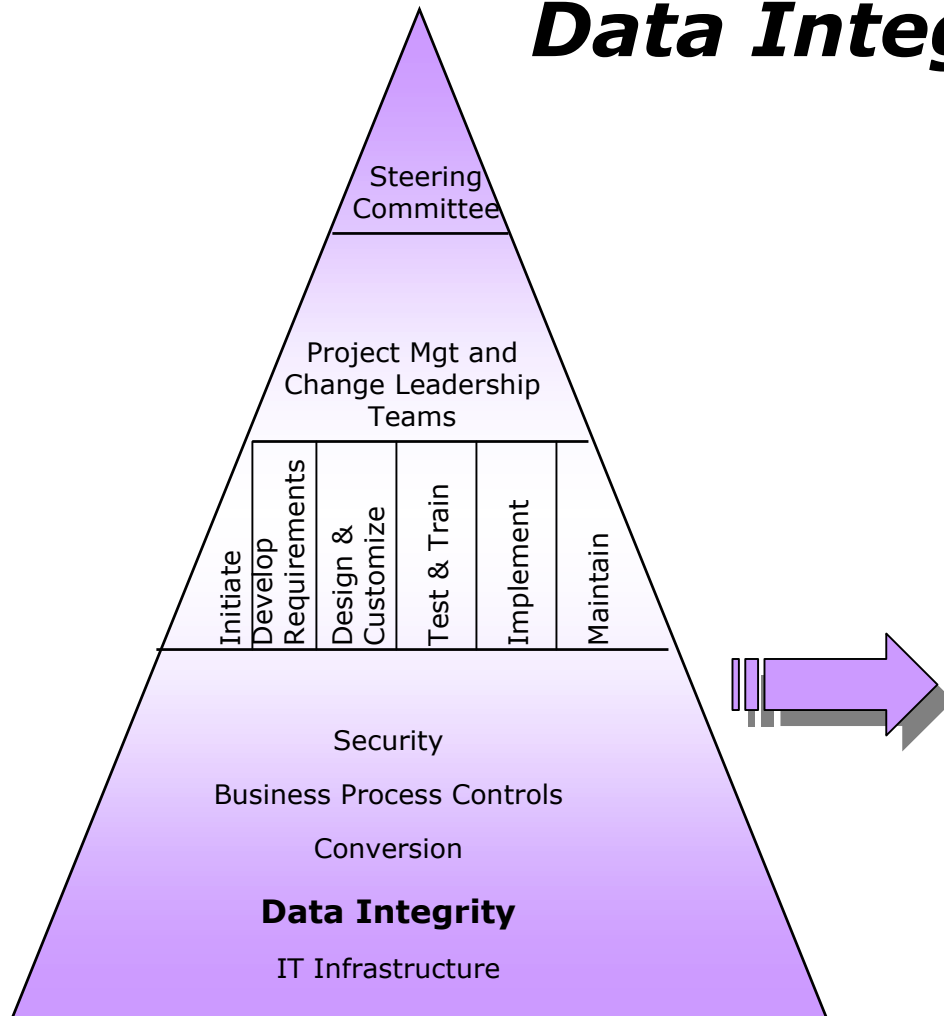
Conversion Controls are initiated, developed, designed, tested and implemented parallel to application development efforts if the project includes a data conversion. Controls include:

- Conversion planning
- Business process mapping
- User involvement in data mapping and data validation activities
- Data analysis and cleansing
- Exceptions handling
- Balancing reports

Process and system integrity controls are applied to every phase of the System Development Life Cycle



Process & System Integrity Controls – Data Integrity

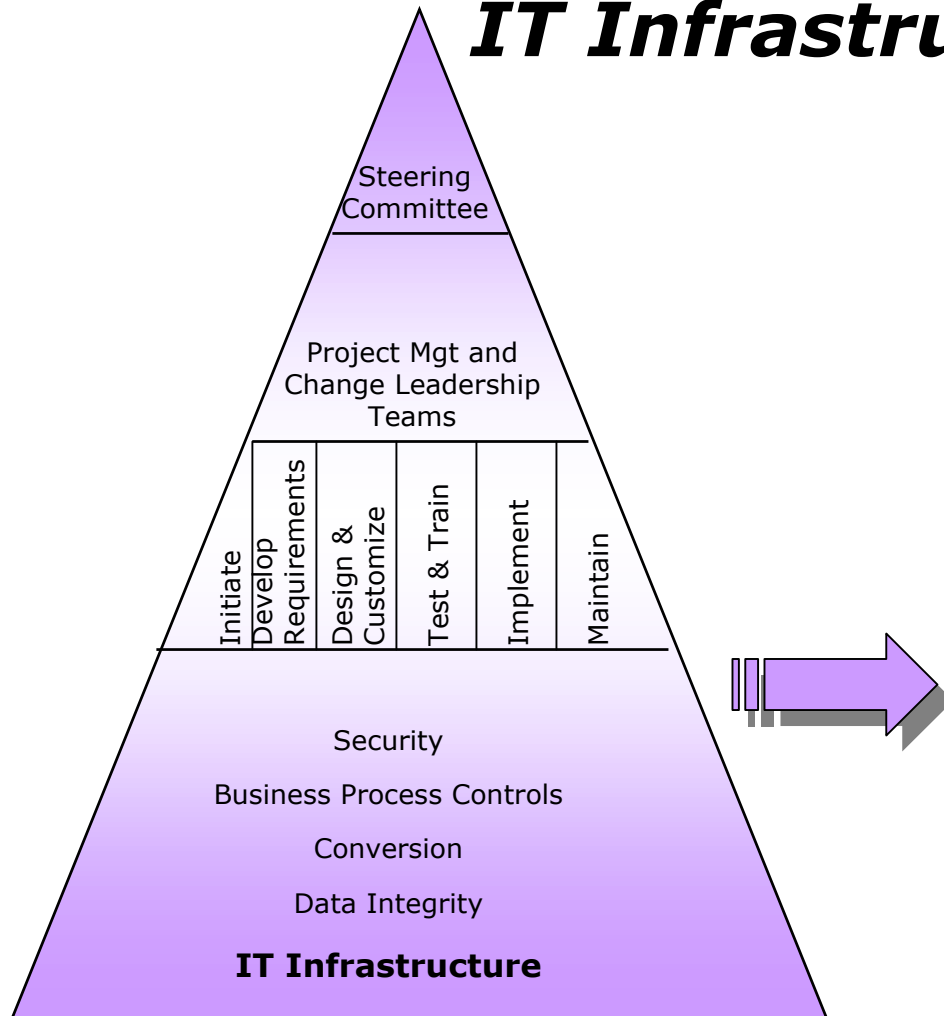


Data Integrity Controls are built into application, interface and conversion design. All data integrity controls should be tested as part of routine Test procedures. Controls include:

- Field edit checks
- Exception reports on key fields in applications and interfaces
- Suspended transactions checks and reports
- Duplicate record / data checks

Process and system integrity controls are applied to every phase of the System Development Life Cycle

Process & System Integrity Controls – IT Infrastructure

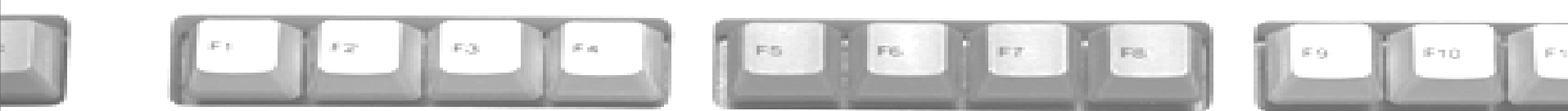


IT Infrastructure Controls should be built into the overall business process through every phase of the SDLC.

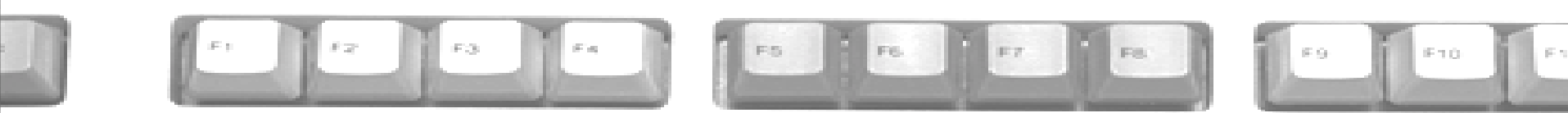
Controls include:

- Data & backup recovery processes for all environments
- System monitoring procedures
- Job scheduling procedures in the mainframe environment
- Application change control procedures
- Help Desk support protocols
- Database configuration control and support
- Capacity planning

Process and system integrity controls are applied to every phase of the System Development Life Cycle



In Conclusion...



In Review

IT Risk Management is the process whereby risk is mitigated in the IT environment.

Project Risk Management is an IT Risk function and includes policies and procedures for:

- Project Management
- System Development Life Cycle
- IT Change Management
- Quality Management
- Management & Oversight

Process and System Integrity Controls are implemented with each PRM policy and procedure. Controls include:

- Security
- Business Processes
- Conversion / Data Integrity
- IT Infrastructure



In Review Cont.

IT Auditors audit for both PRM Policies and Procedures and for the Process and System Integrity controls built into policies and procedures.

The System Development Life Cycle is a Project Risk Management policy and includes procedures for controlling projects through the Project Life Cycle:

- Initiate
- Develop Requirements
- Design and Customize
- Test & Train
- Implement
- Maintain

Process and system integrity controls are built into each phase of the SDLC.



Questions