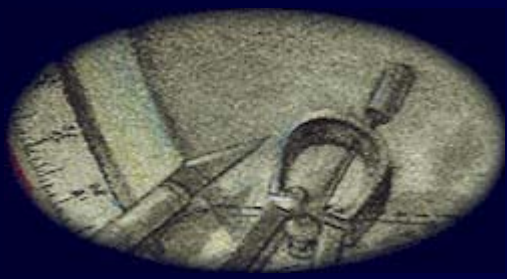# *Risk-Based Security Initiatives*

J. R. Wade, CISSP

Risk-based Security Initiatives

Overview

- **Background**

- **New Information Security Policy framework**

- **New Security Architecture**

- **New Information Security Risk Management Model**
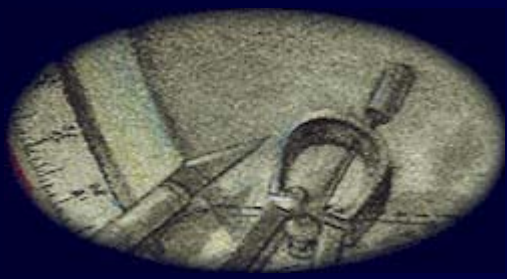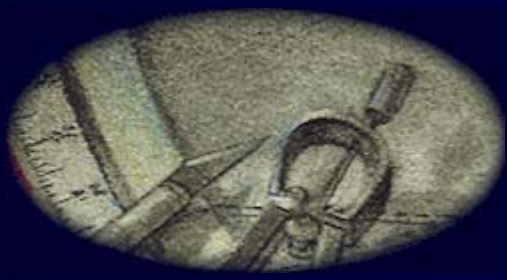
- **Bringing it all together**

Risk-based Security Initiatives - Background

- **Legacy IT environment**
  - inflexible
  - redundant
  - inconsistent
  - single risk view
- **Need to make IT more cost-effective**
- **Responsive to national businesses**
- **Simplify deployment - use standards**
- **Baseline & standardize infrastructure**
- **Consistent approach**

The Blueprint Framework

Development Services

- Application Type & Style
- Code Management
- Language Services
- Libraries
- Project Management
- Quality Assurance & Testing
- Requirements & Modeling

Application Services

- Application Interface
- Business Logic
- System Integration
- System Interface

Data Services

- Authoring (Document & Multimedia Content)
- Data Movement & File Transfer
- Database and Objectbase
- Document and Records Management
- Image Capture & OCR
- Inquiry, Analysis, & Information Discovery
- Metadata
- Report Creation and Distribution
- Search
- Streaming Media
- Web Content Management

Network Based Services

- Address and Directory
- Caching
- Calendaring
- Collaboration
- E-mail and Messaging
- Fax
- File and Print
- Portals and Personalization

Network Services

- External Business Partner & Public Connectivity - Extranet & Internet
- LAN & Facility Backbone - Campus Access
- Mobile, & Telecommuter - Remote Access
- WAN
- Wireless

Platform Services

- Client
- Server
- Storage

Operations Services

- Business Continuity & Disaster Recovery
- Communication
- Deployment
- Management
- Optimization

Security Services

- Authorization
- Confidentiality
- Identification and Authentication
- Integrity
- Availability
- Non-repudiation

4

Standards Taxonomy

Architecture
Orderly arrangement of parts; structure.

Principles
A basic truth, law, or assumption. A rule, especially of good behavior.

Vision
The way in which one sees or conceives something.

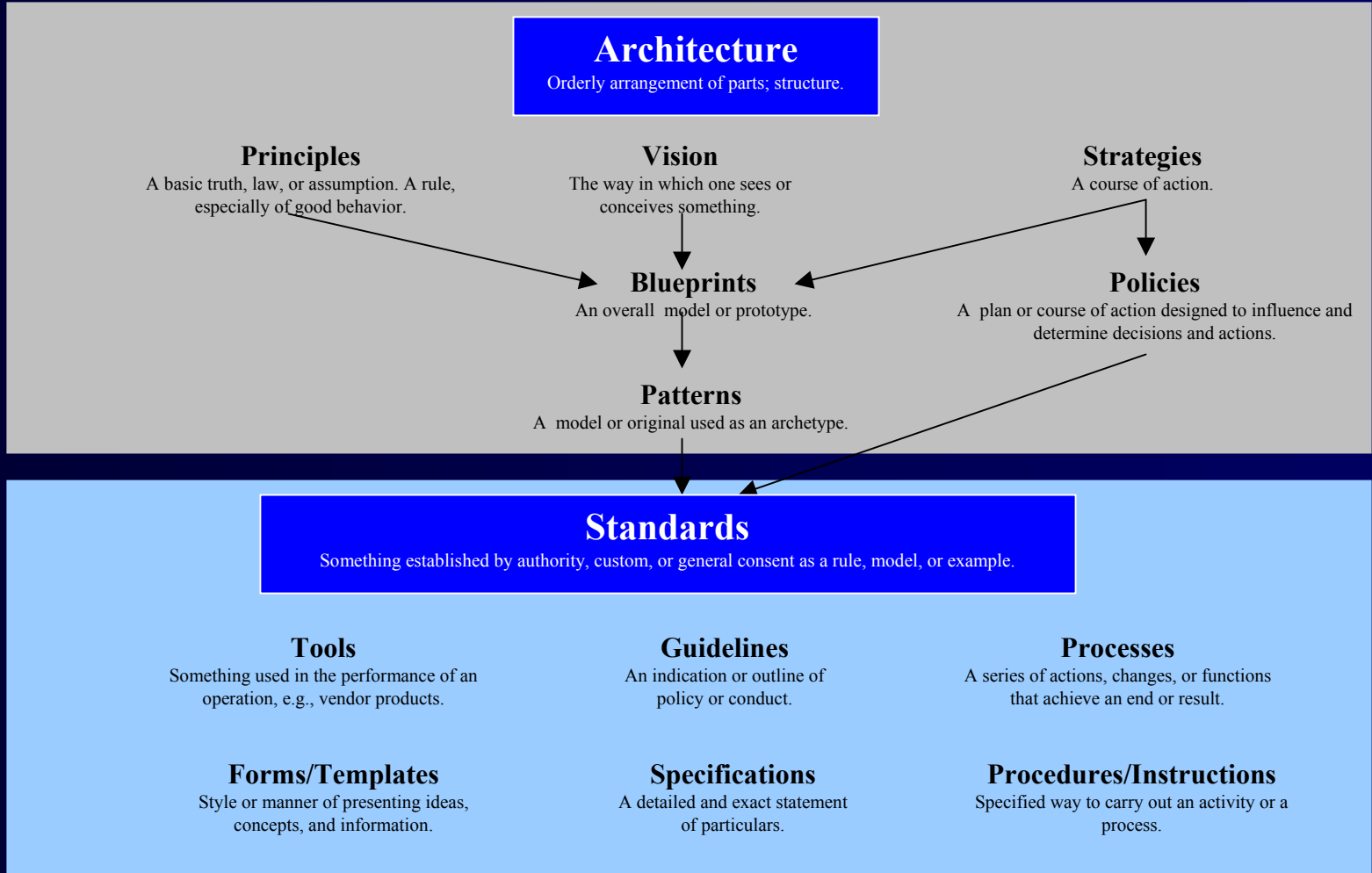**Strategies**
A course of action.

Blueprints
An overall model or prototype.

Policies
A plan or course of action designed to influence and determine decisions and actions.

Patterns
A model or original used as an archetype.

Standards
Something established by authority, custom, or general consent as a rule, model, or example.

Tools
Something used in the performance of an operation, e.g., vendor products.

Guidelines
An indication or outline of policy or conduct.

Processes
A series of actions, changes, or functions that achieve an end or result.

Forms/Templates
Style or manner of presenting ideas, concepts, and information.

Specifications
A detailed and exact statement of particulars.

Procedures/Instructions
Specified way to carry out an activity or a process.

Information Security Policy Framework

Principles ➡ **Management statements of intent for accessing or using information assets**
- What & Why -

Technology Neutral
Adaptable
Consistent Approach ⬅ **Practices** ➡ **Define controls that support Principles**
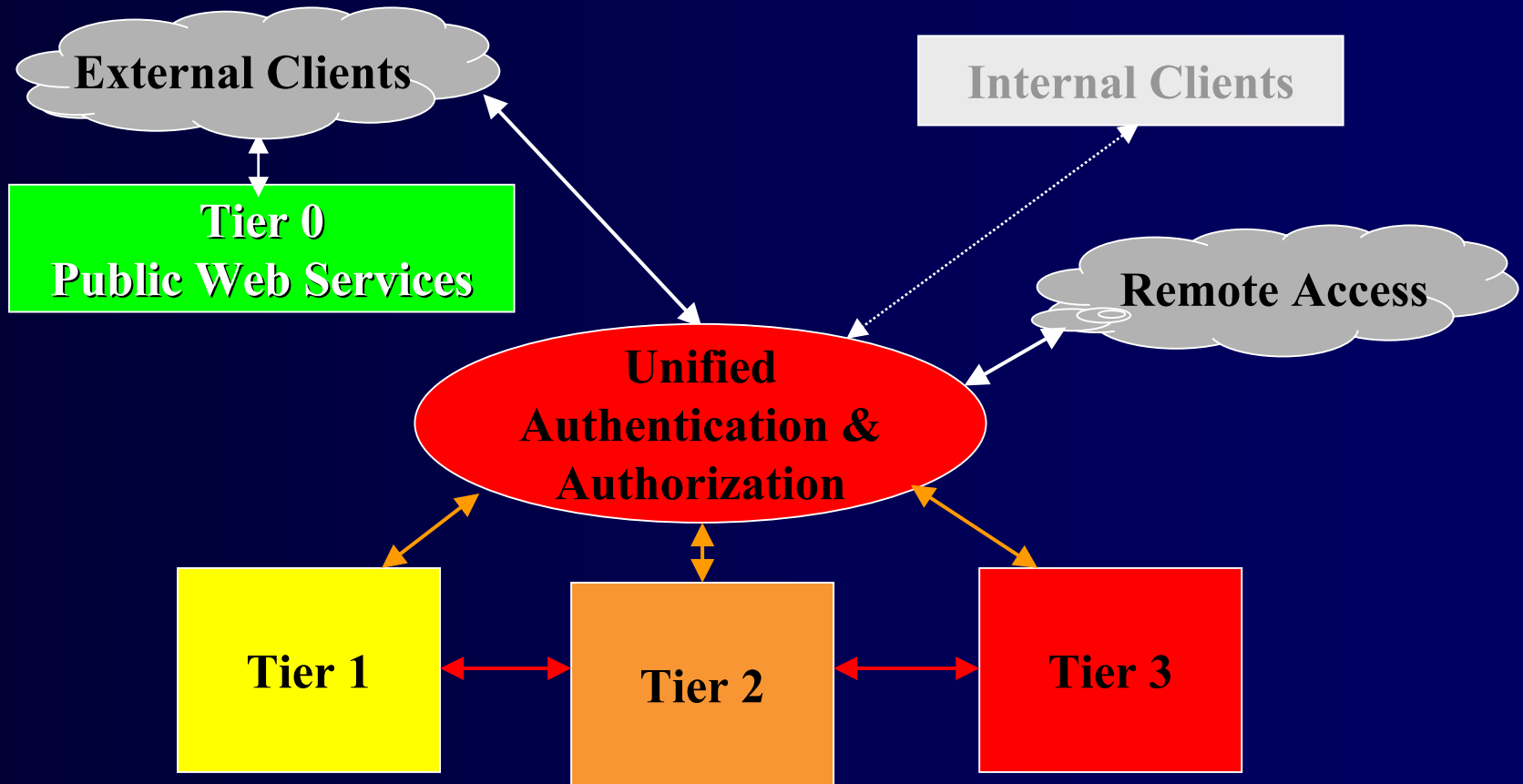**- When, Where, & Who**

How to configure, deploy & secure
a specific technology &/or process
- How - ⬅ **Standards**

New Security Architecture

External Clients

Internal Clients

Tier 0
Public Web Services

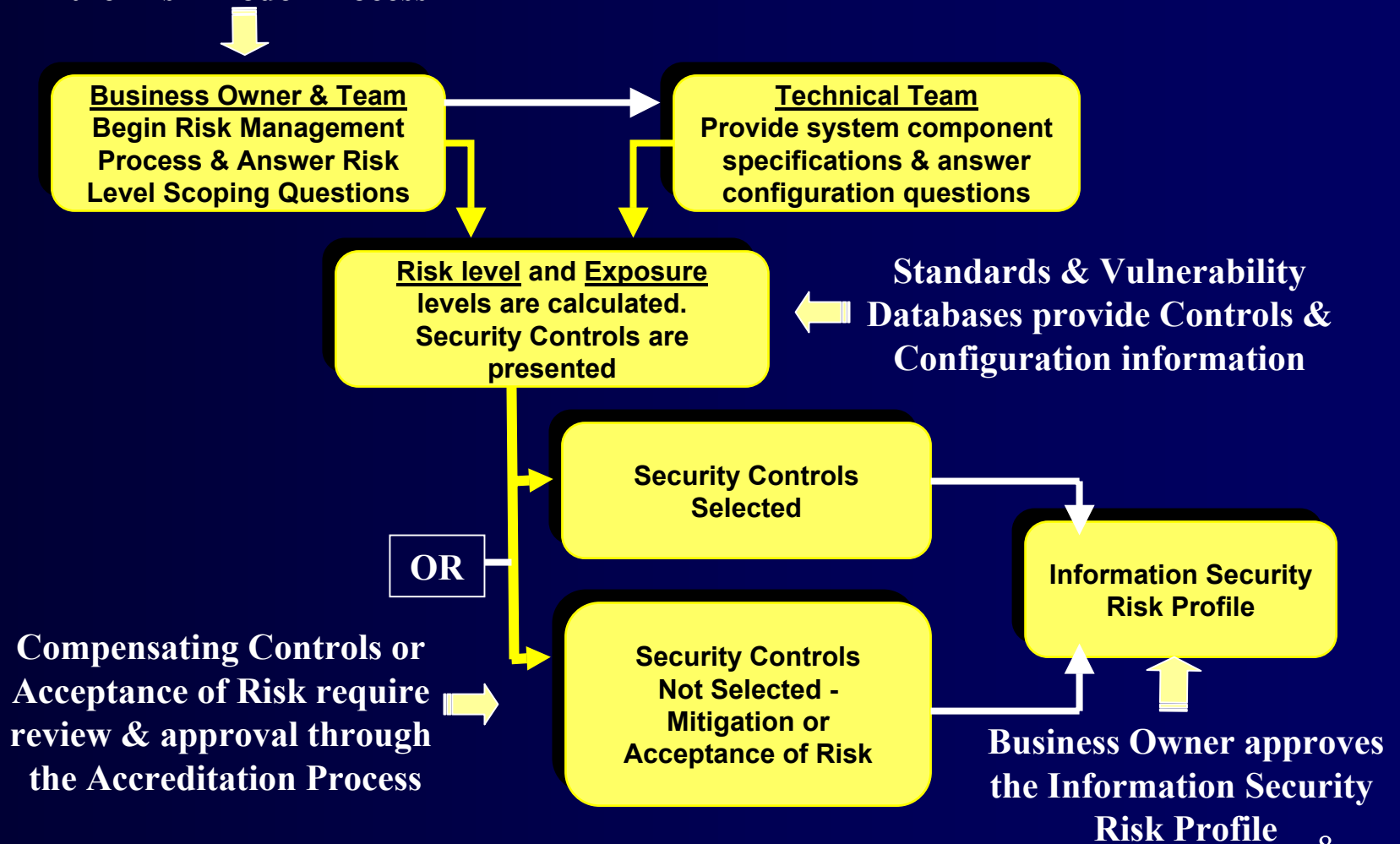Remote Access

Unified
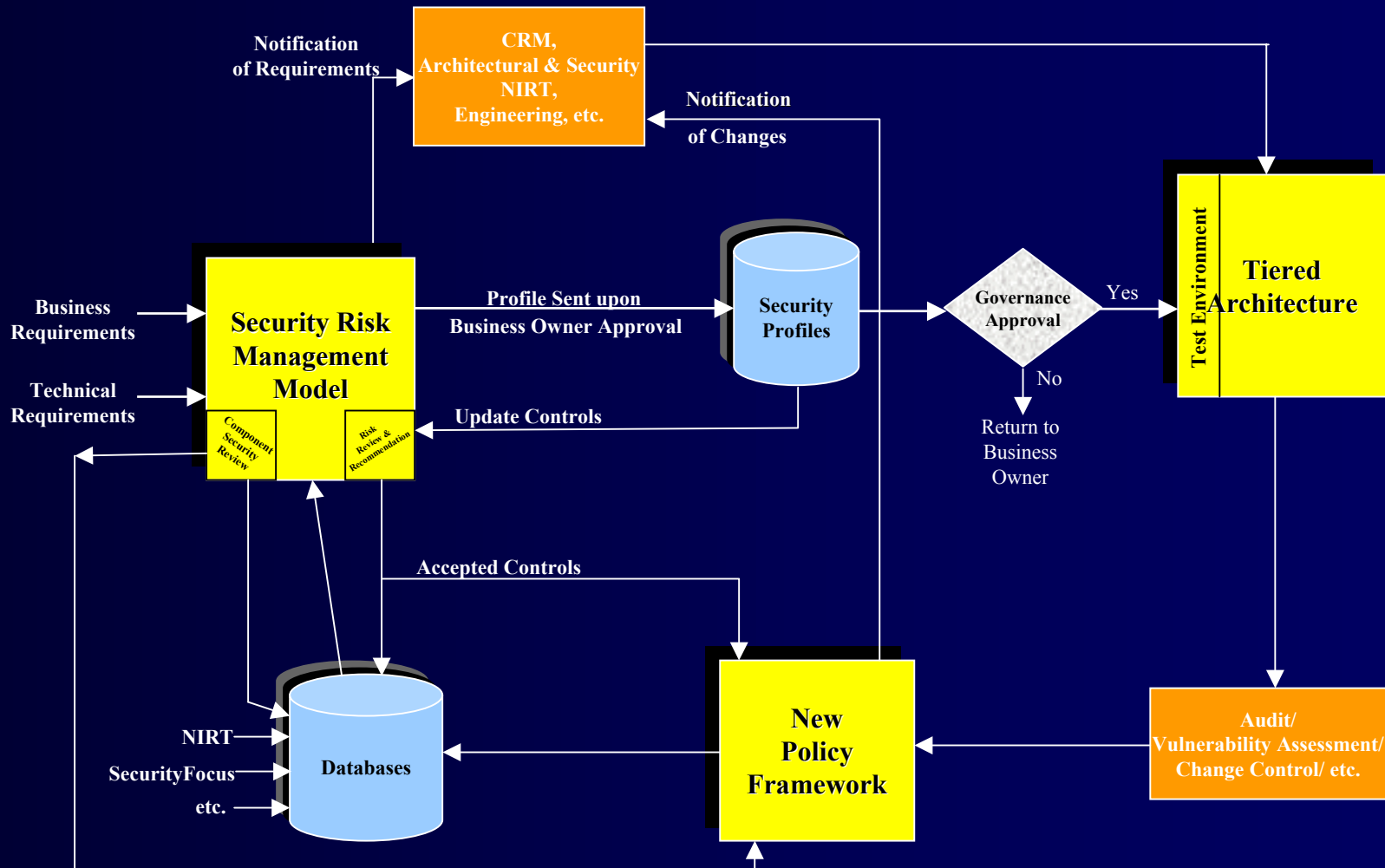Authentication &
Authorization

Tier 1

Tier 2

Tier 3

Pre-defined environments based on risk tolerance.

Information Security Risk Management Model

Business Owner initiates the Risk Model Process

Business Owner & Team
Begin Risk Management Process & Answer Risk Level Scoping Questions

Technical Team
Provide system component specifications & answer configuration questions

Risk level and **Exposure** levels are calculated. Security Controls are presented

Standards & Vulnerability Databases provide Controls & Configuration information

Security Controls Selected

OR

Security Controls Not Selected - Mitigation or Acceptance of Risk

Information Security Risk Profile

Compensating Controls or Acceptance of Risk require review & approval through the Accreditation Process

Business Owner approves the Information Security Risk Profile

8

Risk-based Security Initiatives - Overview

Notification of Requirements

CRM, Architectural & Security NIRT, Engineering, etc.

Notification of Changes

Business Requirements

Technical Requirements

Security Risk Management Model

Component Security Review

Risk Review & Recommendation

Profile Sent upon Business Owner Approval

Security Profiles

Update Controls

Governance Approval

Yes

No

Return to Business Owner

Test Environment

Tiered Architecture

NIRT

SecurityFocus

etc.

Databases

Accepted Controls

New Policy Framework

Audit/ Vulnerability Assessment/ Change Control/ etc.

9