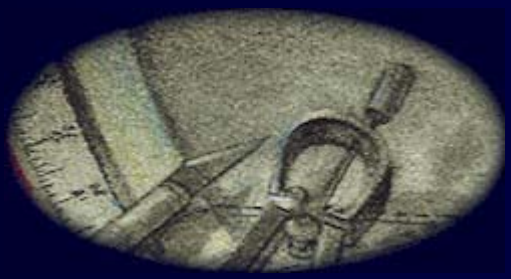
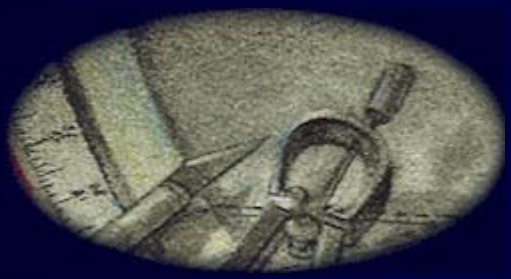


Risk-Based Security Initiatives

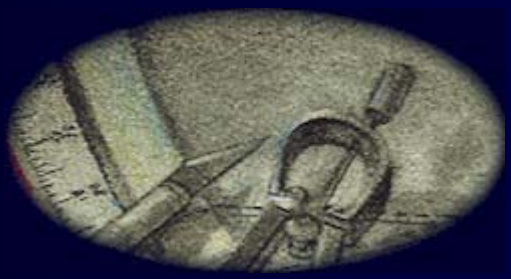
J. R. Wade, CISSP



Risk-based Security Initiatives

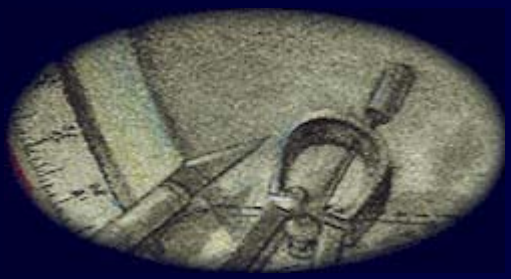
Overview

- 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 - inconsistent
  - redundant - 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

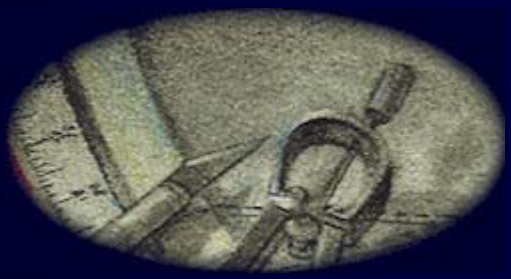
- Client
- Server
- Storage

Operations Services

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

Security Services

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



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.

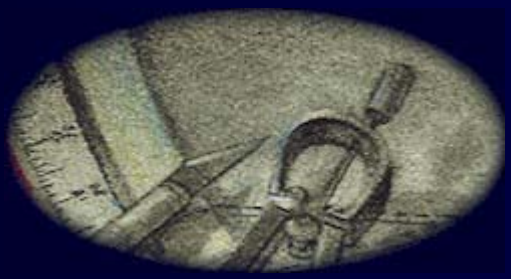
Guidelines
An indication or outline of policy or conduct.

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 -

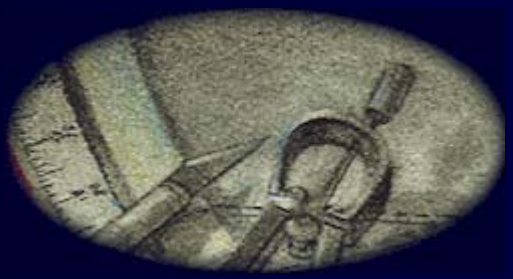
Practices

Technology Neutral
Adaptable
Consistent Approach

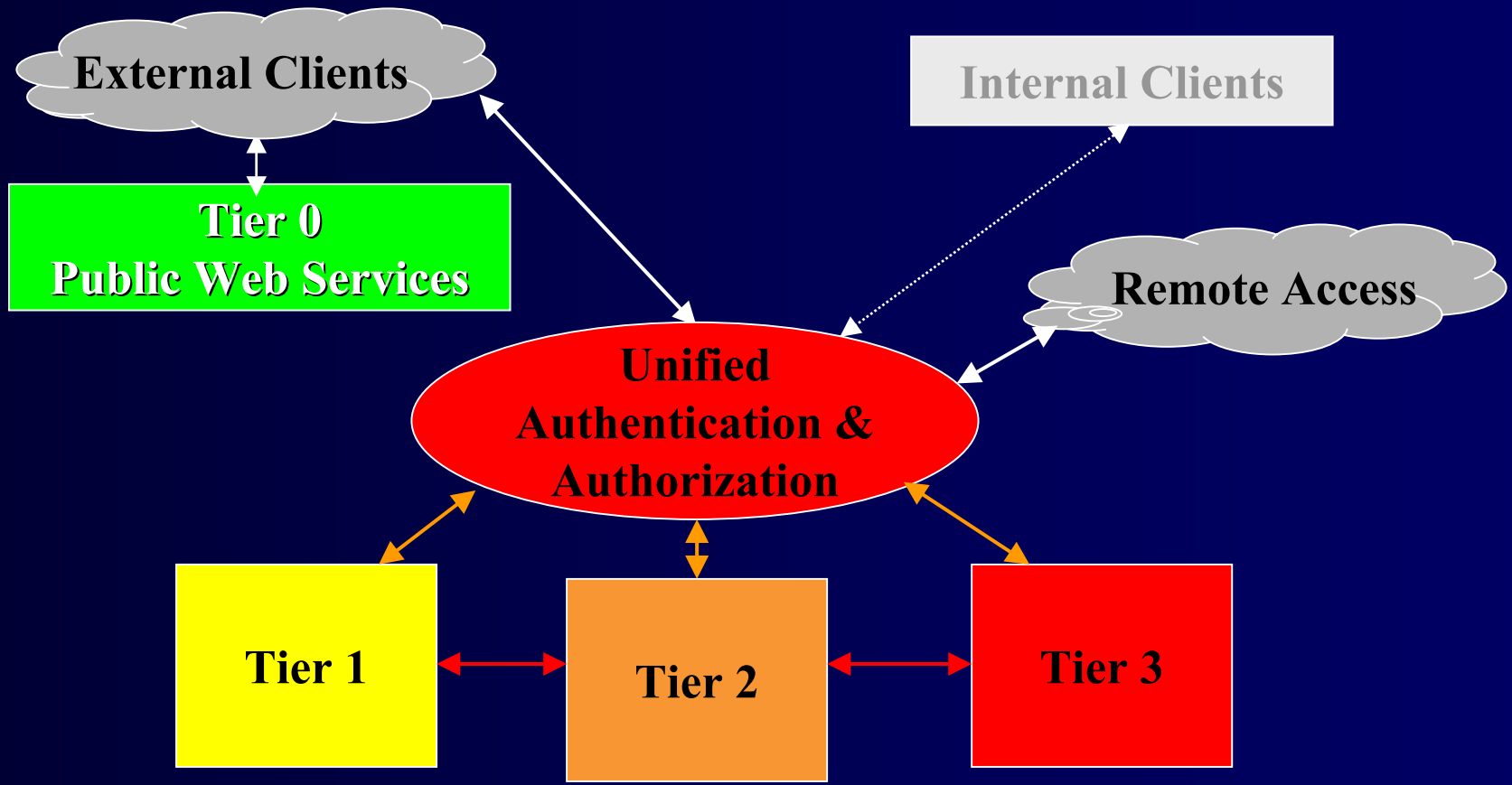
Define controls that support Principles
- When, Where, & Who

Standards

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



New Security Architecture



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

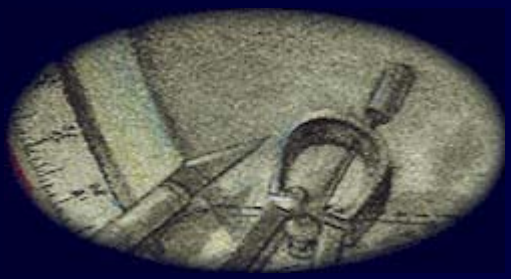
OR

Security Controls Not Selected - Mitigation or Acceptance of Risk

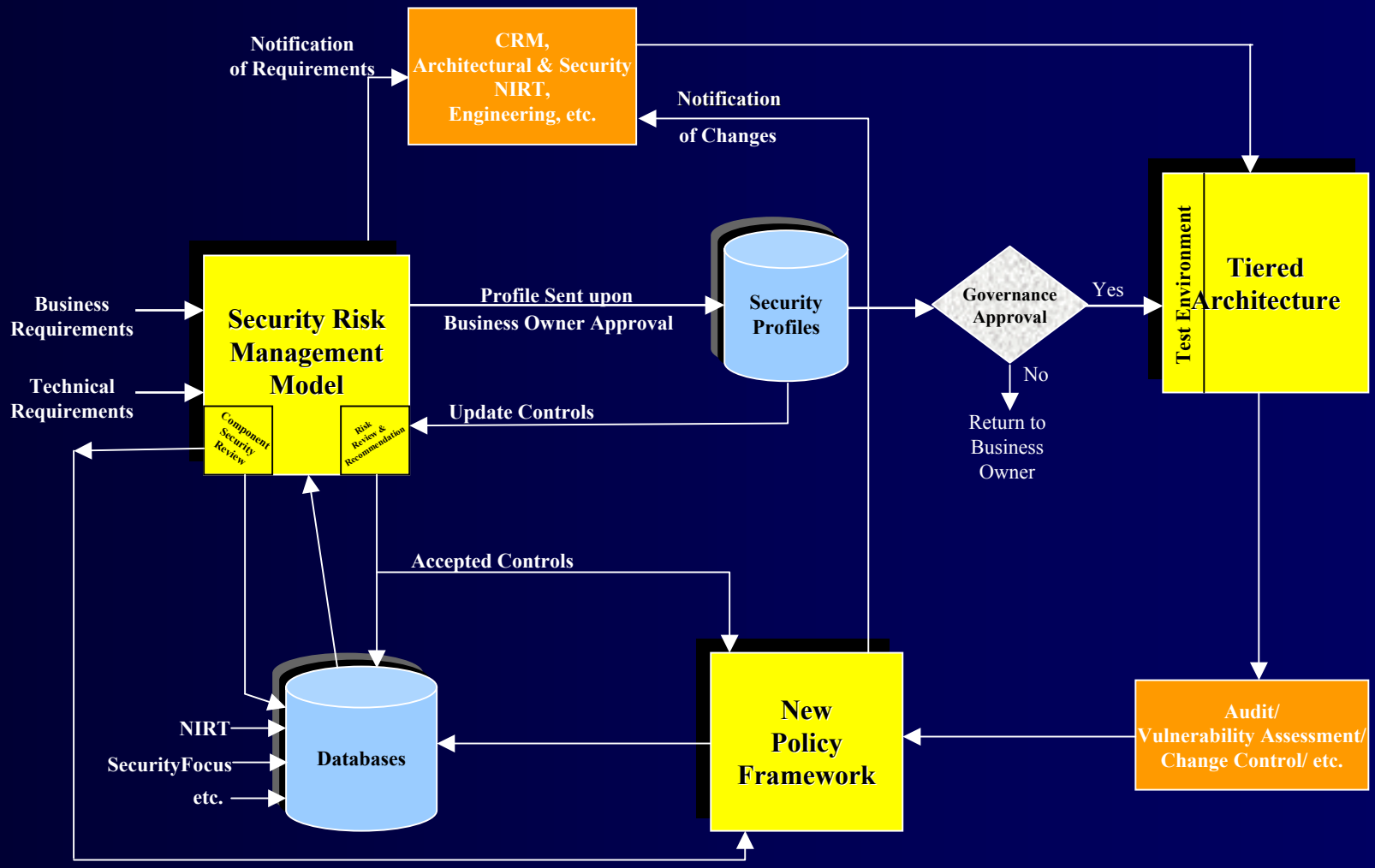
Compensating Controls or Acceptance of Risk require review & approval through the Accreditation Process

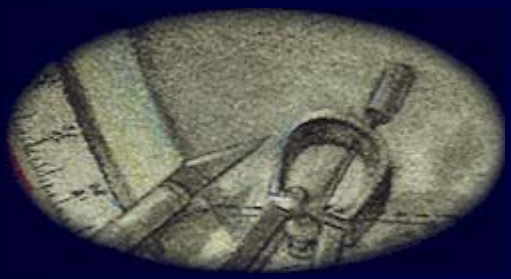
Information Security Risk Profile

Business Owner approves the Information Security Risk Profile



Risk-based Security Initiatives - Overview





Questions?