

# OWASP IL Mini Conference 2007

## Application Security not just development

David Lewis, CISM, CISA, CISSP  
Information Security Services Lead  
Rosenblum Holtzman

**May 21, 2007**

# Objective

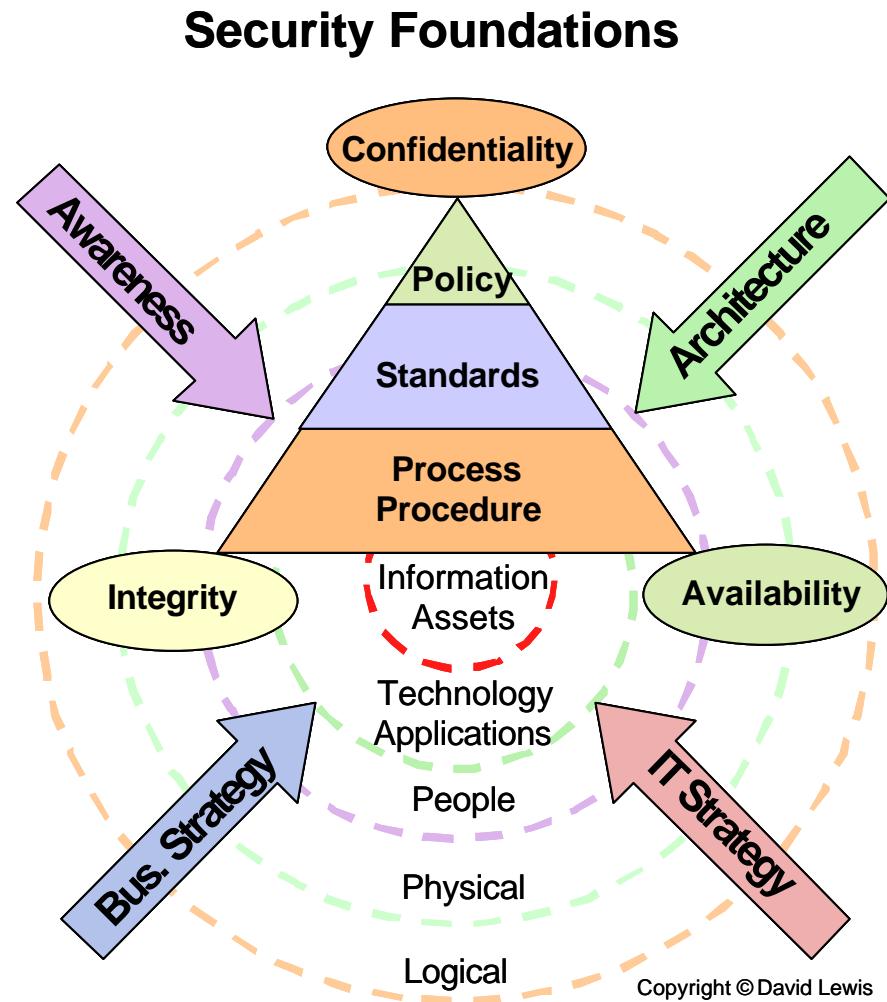
- To provide developers with a broader view of security and controls than just their secure coding environment

# Agenda

- What is an Information Asset
- Information Security relevance to Developers
- Control Frameworks
- Controls divided into 3 categories
- Responsibilities
- Help Available

# What is an information Asset?

- Information that has a value can be considered an Information Asset
- This includes all types of information including files, databases, paper-based and electronic documents, records, hardware items, software or other infrastructure items



# How is Application Development relevant to Information Asset protection?

- Regulations and standards demand controls
  - SOX, PCI, 52-111, HIPAA, PIPEDA, BASIL II, ISO 17799, COBIT
- Applications provide a layer of security for Information Assets, one of many layers
  - Cost of adding this later is 98c as compared to 2c in the beginning
- Weak security architecture could lead to major project delays if not scrapped completely
  - See FBI Virtual Case File (VCF) failure
    - <http://archives.neohapsis.com/archives/isn/2002-q4/0090.html>
- Risk management includes Application Security
  - Ensuring business controls are in place around development and the developers

# IEC/ISO 17799-2005 – Security Framework

1. Security Policy
2. Organization of Information Security
3. Asset Management
4. Human Resources Security
5. Physical and Environmental Security
6. Communications and Operations Management
7. Access Control
8. Information Systems Acquisition, Development and Maintenance
9. Information Security Incident Management
10. Business Continuity Management
11. Compliance

Application security is more than just this

# COBIT – 34 Processes

## Planning and Organization

- PO1.0 Define a Strategic IT Plan
- PO2.0 Define the Information Architecture
- PO3.0 Determine Technology Direction
- PO4.0 Define the IT processes, organisation and relationships.
- PO5.0 Manage the IT investment.
- PO6.0 Communicate Management Aims and Objectives
- PO7.0 Manage IT human resources.
- PO8.0 Manage quality.
- PO9.0 Assess and manage IT risks.
- PO10.0 Manage projects.

## Acquisition and Implementation

- AI1.0 Identify automated solutions.
- AI2.0 Acquire and maintain application software.
- AI3.0 Acquire and maintain technology infrastructure.
- AI4.0 Enable operation and use.
- AI5.0 Procure IT resources.
- AI6.0 Manage changes.
- AI7.0 Install and accredit solutions and changes.

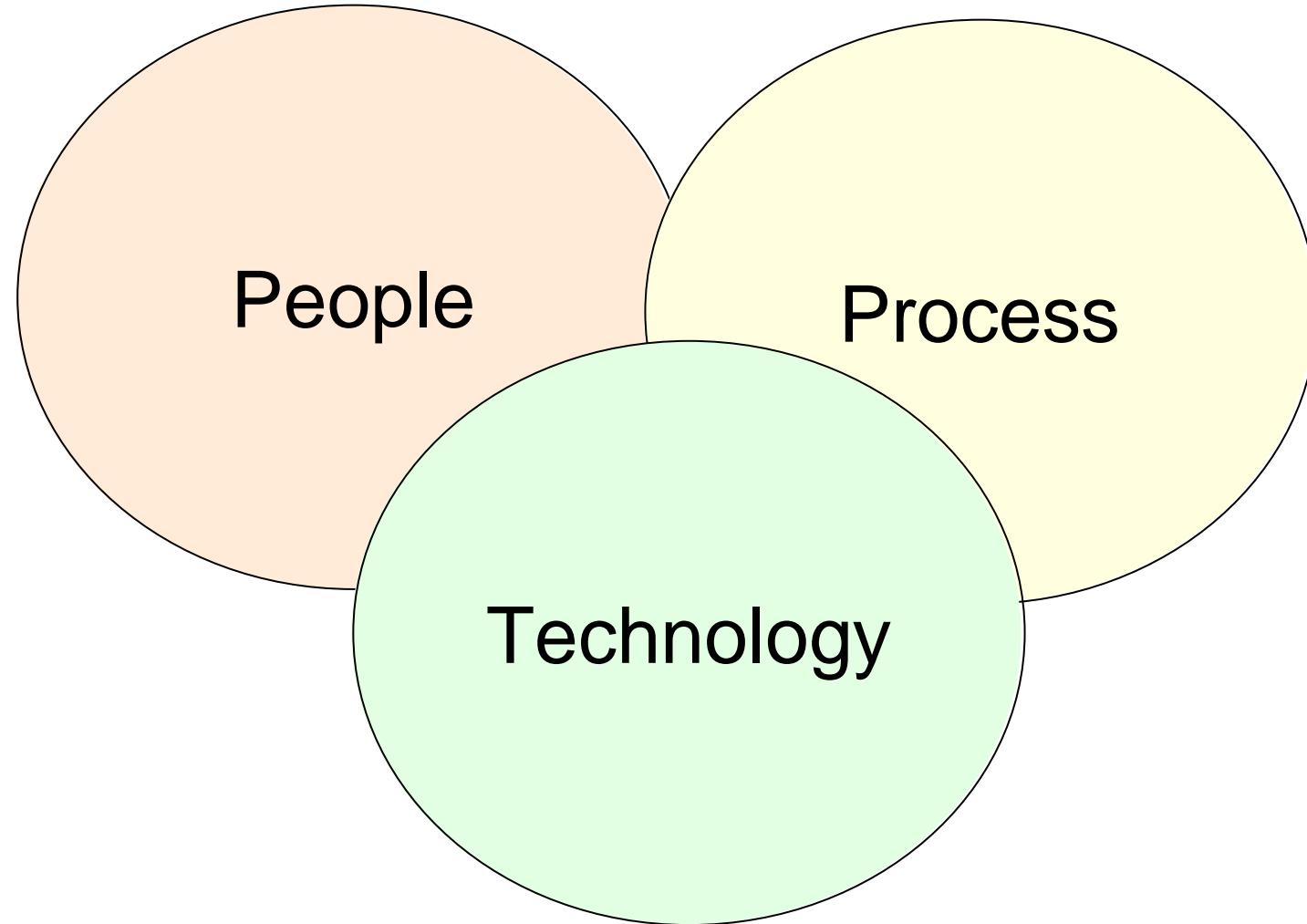
## Delivery and Support

- DS1.0 Define and manage service levels.
- DS2.0 Manage third-party services.
- DS3.0 Manage service delivery and capacity.
- DS4.0 Manage service quality.
- DS5.0 Manage service costs.
- DS6.0 Manage service users.
- DS7.0 Manage service level agreements.
- DS8.0 Manage problems.
- DS9.0 Manage data.
- DS10.0 Manage the physical environment.
- DS11.0 Manage operations.

## Monitor and Evaluate

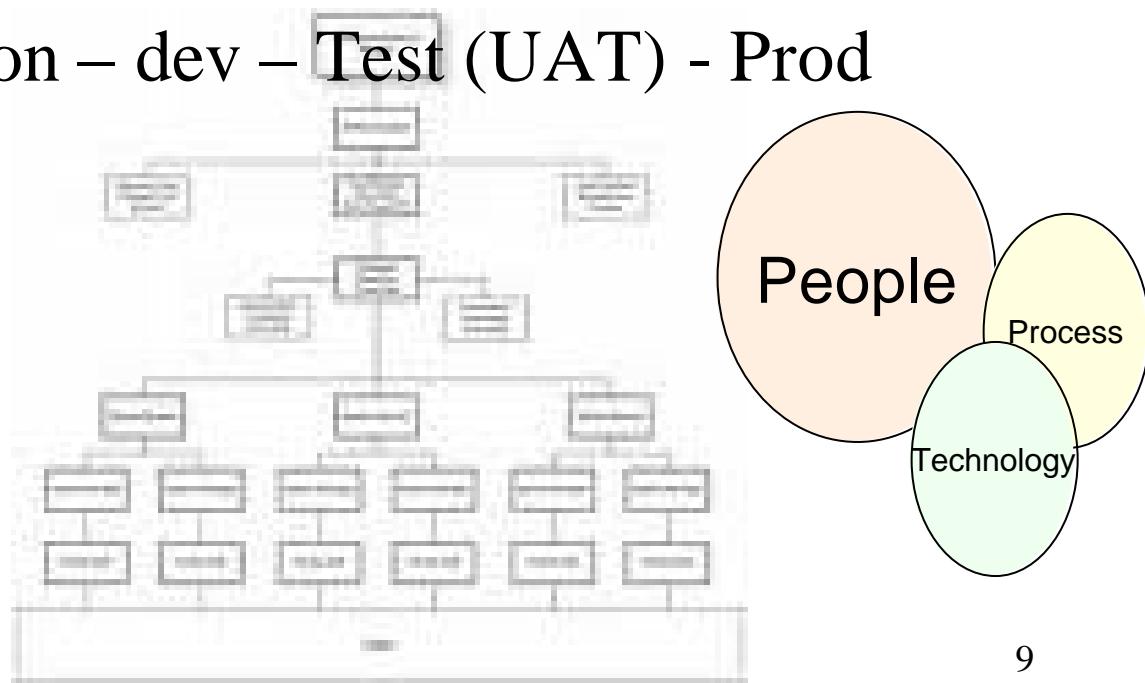
- ME1.0 Monitor and evaluate IT performance.
- ME2.0 Monitor and evaluate internal control.
- ME3.0 Ensure regulatory compliance.
- ME4.0 Provide IT governance.

# Breaking down controls into 3 Categories



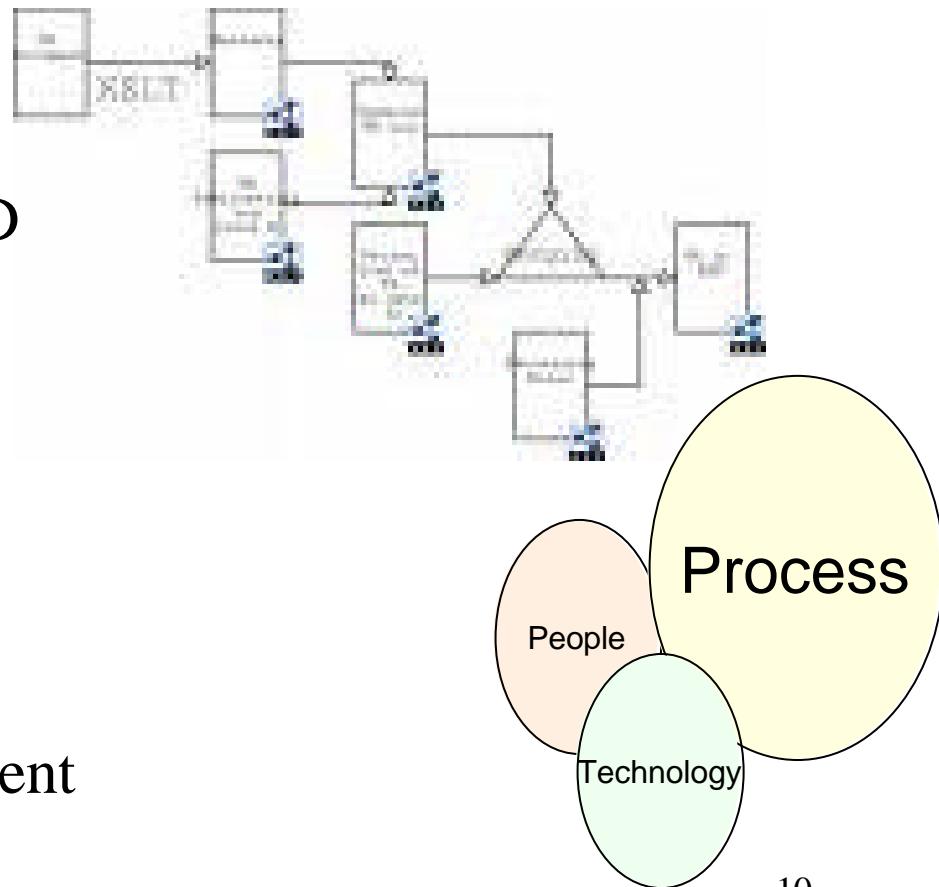
# People

- User Awareness is KEY
- Training based functions being performed
- Responsibilities
  - Code migration – dev – Test (UAT) - Prod
  - Testing
  - Signoff
- Outsourcing



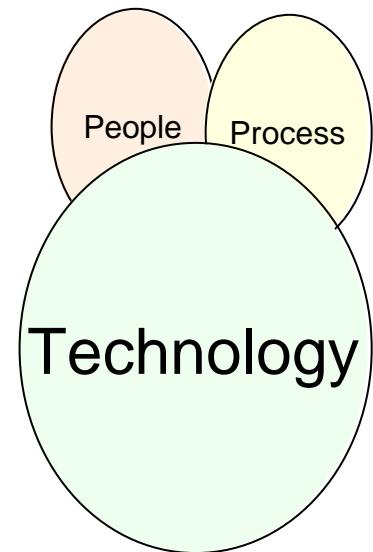
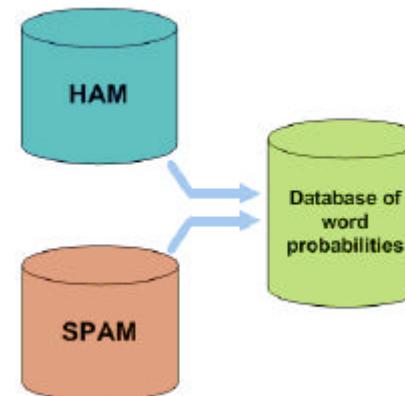
# Process

- Policy and Standards driving security
- Processes for
  - Change management
  - Access Control – MACD
  - Documentation
  - Testing
  - Backup and restore
  - Migration of code
  - Version control
  - Assurance/Self Assessment



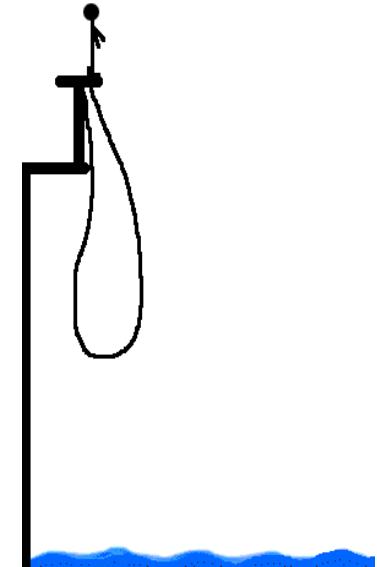
# Technology

- Secure Development environment
  - As secure as production
- Separate network from test and production
- Restricted access to code
  - On a need to know
- Logging and auditing in place
- Testing
  - Web application testing
  - Automated code review
- Data base security



# Who's is responsible?

- Executive
  - Developing culture and principles
  - Reporting to board, shareholders, investors
  - Attest to meeting control requirements
  - Sign off
- Risk Management/Governance
  - Developing and providing controls
  - Validating controls are in place
- Lines of Business
  - Understanding and implementing
  - Self analysis
- AS well ... **YOU!!!**



- Understanding
- Executing
- Confirming

# Help with Information Security risks and controls?

- Consulting Risk services
- Application Vulnerability Assessment Tools
  - Beyond the standard Ethical hacking tools
- Database Security
  - Protecting the data and access to it
- Application Code review tools
- Auditors (Internal and External)

# Thanks

- If you any questions about your development environments or larger organizational risk I will be happy to speak to you after the conference.

David Lewis, CISM, CISSP, CISA  
Information Security Lead  
Rosenblum Holtzman  
[dmlsec@gmail.com](mailto:dmlsec@gmail.com)  
Tel: 054-7980-307