Ensuring Business Considerations in your Security and Compliance Processes Aka Bringing Methodology Back to Security

Greg Miles, Ph.D., CISSP, CISA, CISM
Program Champion, Cyber Studies
University of Advancing Technology
gmiles@uat.edu

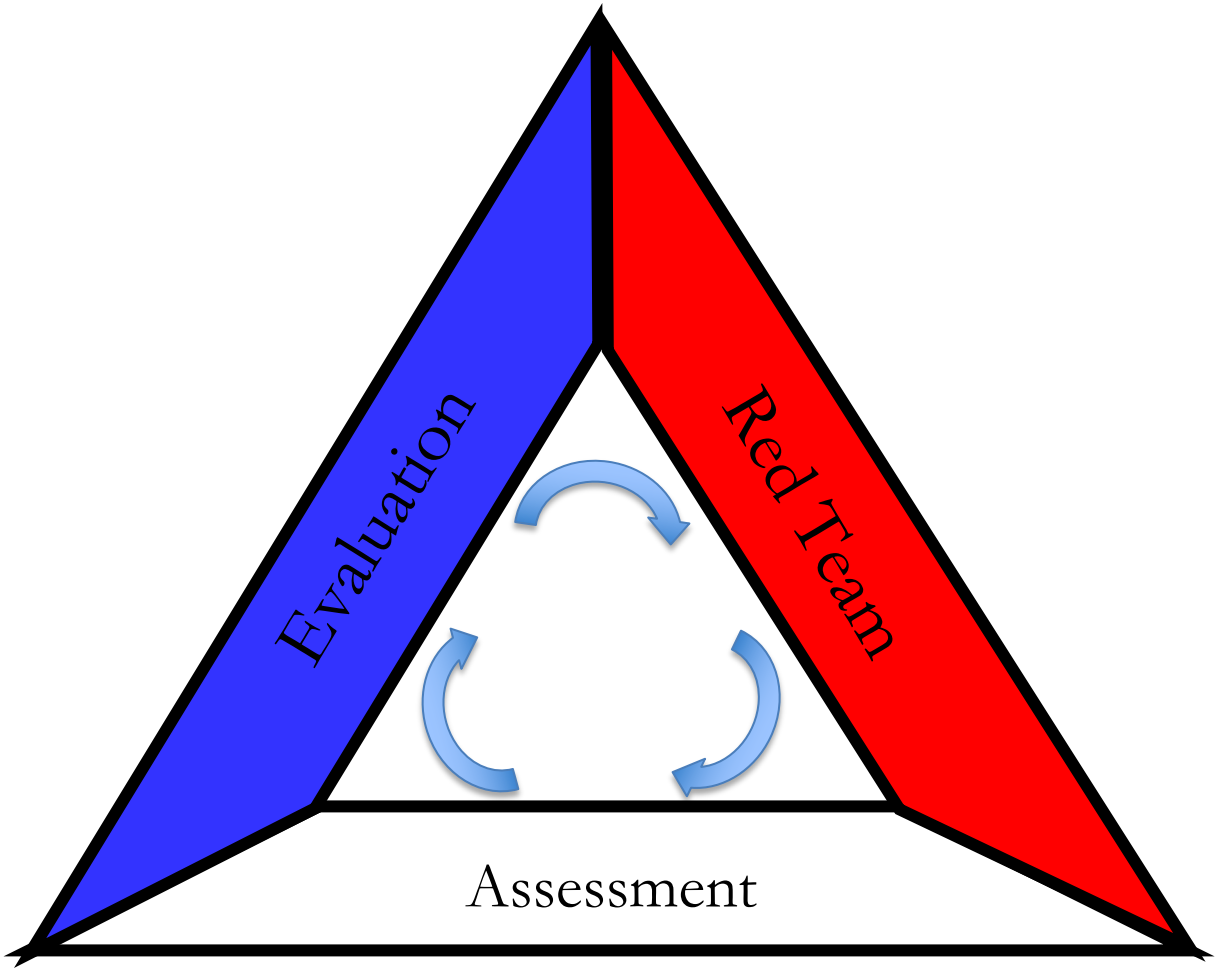
SUCCESSFUL METHODOLOGY

- Methodology must be:
  - Comprehensive
  - Flexible
- Every security program has to relate back to business operations.
  - Includes security objectives
  - Includes compliance objectives
  - Also includes business objectives
- Is everything beyond this "gravy" or a waste of money??

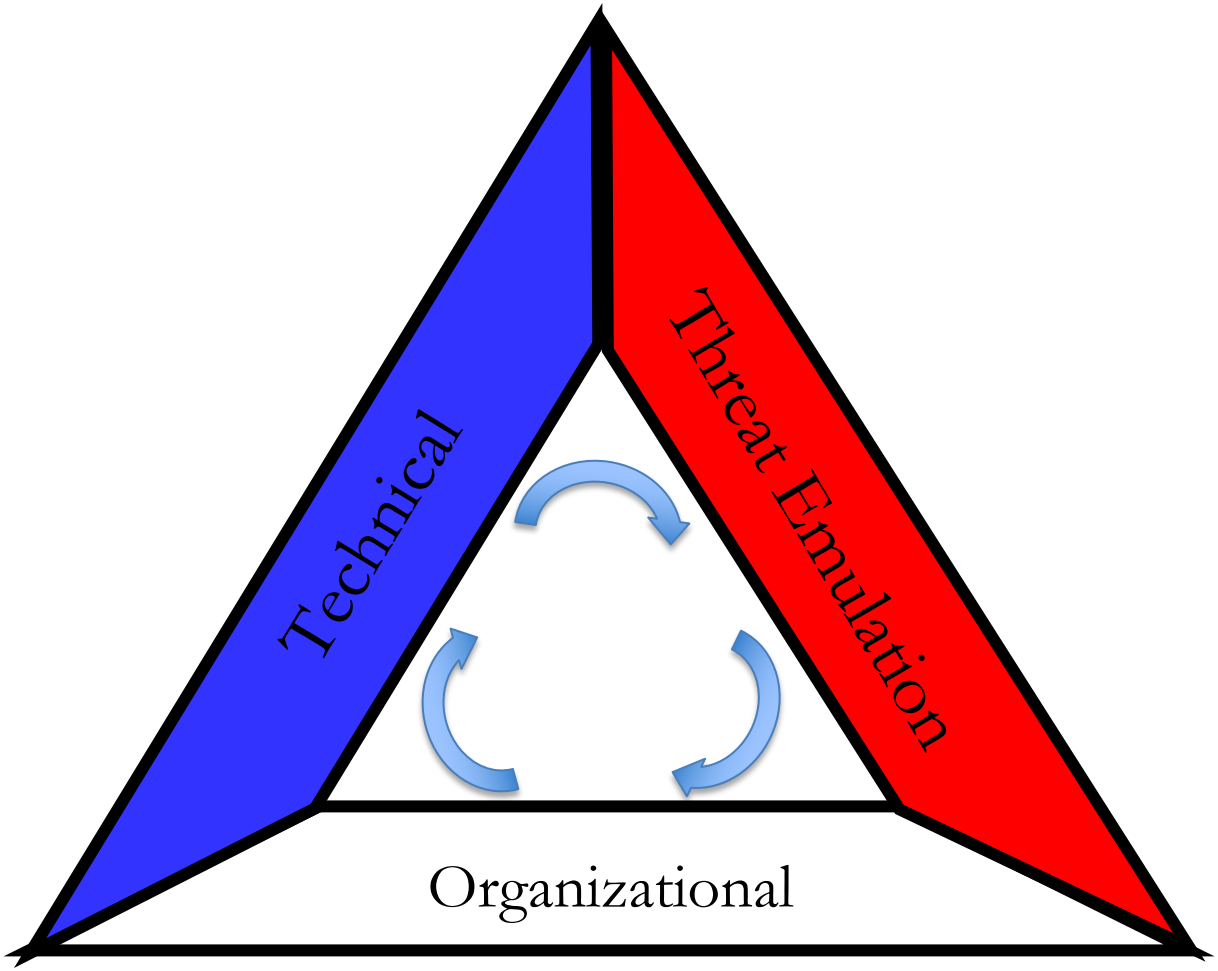
VULNERABILITY DISCOVERY TRIAD

ASSESSMENTS (Level I)	EVALUATIONS (Level II)	RED TEAM (Level III)
- Cooperative High Level Overview - Information/Mission Criticality Analysis - Includes Policy, Procedures, & Information Flow - No Hands-on Testing	- Hands-on process - Cooperative Testing - Diagnostic Tools - Penetration Tools - Specific Technical Expertise	- Adversarial - External Penetration Tests - Simulation of Appropriate Adversary

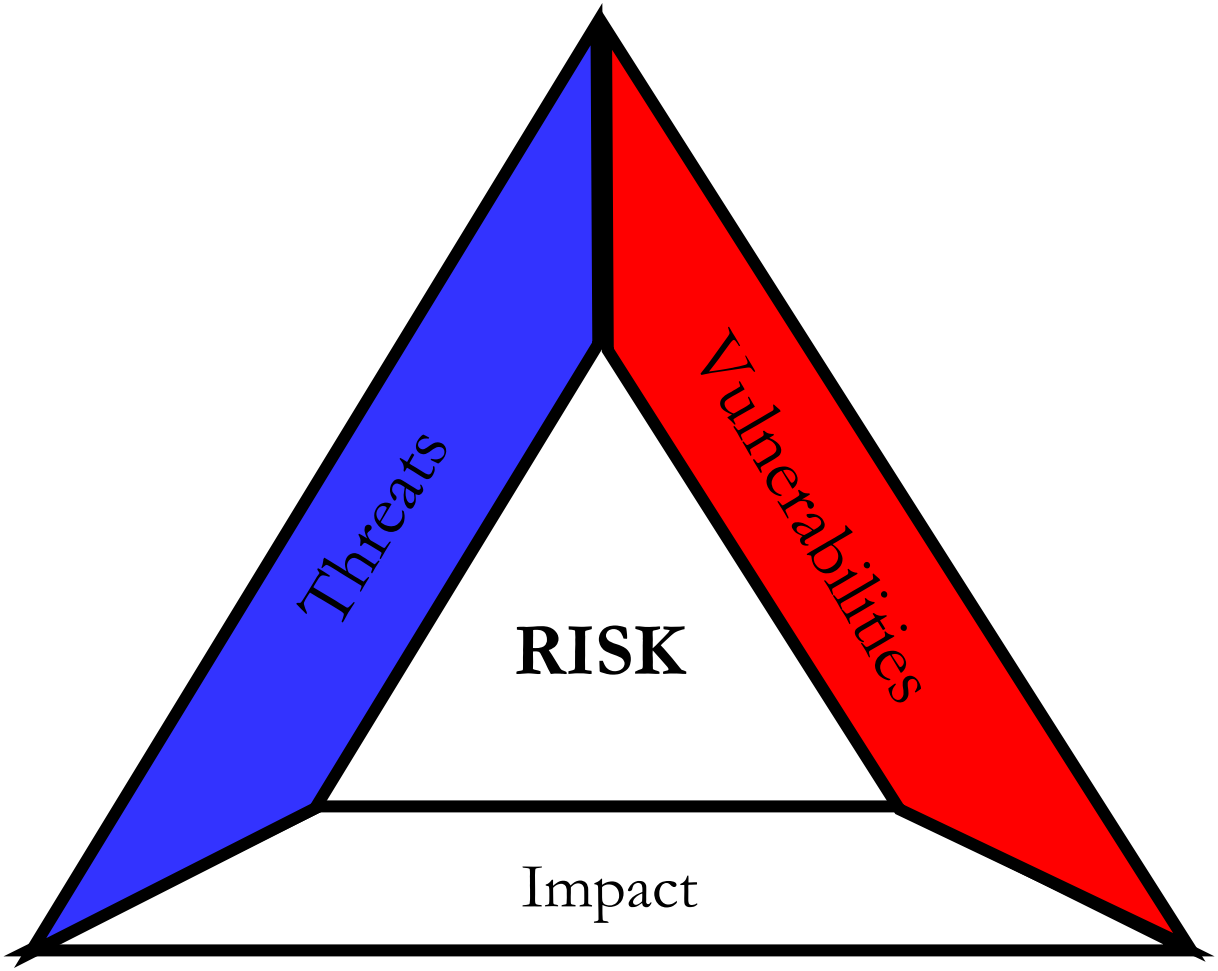
VULNERABILITY DISCOVERY TRIAD



SECURITY AND COMPLIANCE PROCESS



POWER OF THE TRIANGLE



ORGANIZATIONAL PROCESS

- Define and Understand Business Processes
- Define and Understand Compliance Requirements
- Define and Understand Governance Requirements
- Define and Understand the Critical Business Information Needed To:
  - Accomplish Business Goals and Objectives
  - Perform Business Functions and Requirements
  - Meet Stakeholder Needs
- Define and Document the Impact and Thresholds within the Business Operations

ORGANIZATIONAL PROCESS

- Identify and Document the Systems that Process, Transmit and/or Store Critical Business Information
- Determine the Security Posture Objectives
- Perform a Gap Analysis of Objectives against Current State

- Make Improvements

ORGANIZATIONAL PROCESS

Also Considered:

- Full Range of Documentation and Actions
  - Security Program
  - Incident Response
  - Crisis Management
  - Business Continuity/Disaster Recovery
  - Change Control
  - Network and Security Operations
  - Other Policy and Procedural Documentation
- Education, Training and Awareness
- Annual Testing of Procedures
- Threat Determination

ORGANIZATIONAL PROCESS

Critical Business Information and Impacts

Gap Analysis and Mitigation Plan

Compliance and Governance Requirements

PROGRAM COMPONENTS ORGANIZATIONAL

Management

1. PROGRAM MANAGEMENT (PM)
2. SECURITY ASSESSMENTS AND AUTHORIZATION CONTROLS (CA)
3. PLANNING (PL)
4. RISK ASSESSMENT (RA)
5. SYSTEM AND SERVICES ACQUISITION (SA)

Operational

6. AWARENESS AND TRAINING (AT)
7. CONFIGURATION MANAGEMENT (CM)
8. CONTINGENCY PLANNING (CP)
9. INCIDENT RESPONSE (IR)
10. MAINTENANCE (MA)
11. MEDIA PROTECTION (MP)
12. PHYSICAL AND ENVIRONMENTAL PROTECTION (PE)
13. PERSONNEL SECURITY (PS)
14. SYSTEM AND INFORMATION INTEGRITY

Technical

15. ACCESS CONTROL (AC)
16. AUDIT AND ACCOUNTABILITY (AU)
17. IDENTIFICATION AND AUTHENTICATION (IA)
18. SYSTEM AND COMMUNICATIONS PROTECTION (SC)

TECHNICAL PROCESS

Organizational Process Feeds the Technical Process

- Prioritizes Systems based on Criticality for Business Operations
- Identifies the Vulnerabilities that can affect Business Operations
- Can Include:
  - Technical Vulnerability Testing (network, host and application)
  - Technical Penetration Testing
  - Physical Penetration Testing
  - Computer Forensics
  - Network Device Analysis

PROGRAM COMPONENTS TECHNICAL

1. Port Scanning
2. SNMP Scanning
3. Enumeration & Banner Grabbing
4. Wireless Enumeration
5. Vulnerability Scanning
6. Host Evaluation
7. Network Device Analysis
8. Password Compliance Testing
9. Application Specific Scanning
10. Network Sniffing

MONITORING

- Implement Continuous Monitoring once you understand what you are supposed to be protecting
- Monitor Critical Business Functions based on the Organizational Process to include:
  - Remediation Plan Status
  - Implementation and Testing of Policies and Procedures
  - Education, Training and Awareness Implementation
  - Changes to Business Operations/Requirements
- Monitor the Critical Technical Functions based on the Organizational and Technical Process to include:
  - Network Devices
  - Critical Technical Systems
  - Firewalls, IDS, IPS

TESTING

- Test Your Critical Policies and Processes (IR, BC/DR etc.)
- Test Your Technical
  - Frequent Vulnerability Scans and Remediation
  - Periodic Red Teaming
    - Penetration Testing
    - Social Engineering

SUMMARY

- Organizational, Technical and Threat Emulation closely tie together to accomplish business, security, compliance and governance requirements.
- The foundation of the security framework is the Organizational Process that maps business requirements and impacts to your required compliance area and security objectives.
- Conducting the Gap Analysis shows strengths and weaknesses in your overall framework.
- Monitor and Test

QUESTIONS?

Greg Miles, Ph.D., CISSP, CISA, CISM
Program Champion, Cyber Studies
University of Advancing Technology
gmiles@uat.edu

UAT Cyber Studies Program
Associates and Bachelor Degree Program Areas:
Cyber Security
Technology Forensics
Network Engineering

Graduate Degree Program Area:
Cyber Security